

特開平8-288940

(43) 公開日 平成8年(1996)11月1日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08		8842-5 J	H 0 4 L 9/00	6 0 1 B
G 0 6 F 15/00	3 3 0	9364-5 L	G 0 6 F 15/00	3 3 0 Z
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 F
		7259-5 J		6 3 0 B
H 0 4 H 1/00			H 0 4 H 1/00	F

審査請求 未請求 請求項の数 8 F D (全 15 頁) 最終頁に続く

(21) 出願番号 特願平7-348095

(22) 出願日 平成7年(1995)12月11日

(31) 優先権主張番号 特願平6-309292

(32) 優先日 平6(1994)12月13日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(72) 発明者 斉藤 誠

東京都千代田区丸の内2丁目6番3号 三

菱商事株式会社内

(72) 発明者 粉木 準一

東京都千代田区丸の内2丁目6番3号 三

菱商事株式会社内

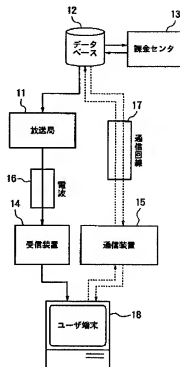
(74) 代理人 弁理士 南條 眞一郎

(54) 【発明の名称】 暗号鍵システム

(57) 【要約】

【課題】 暗号鍵システムの発明をテレビジョンシステム、データベースシステムあるいは電子商取引システム等に適用するための具体的な構成を得る。

【解決手段】 このシステムは放送局、データベース、受信装置、データ通信装置及びユーザ端末装置から構成され、暗号鍵方式としては秘密鍵方式、公開鍵方式、デジタル署名方式が用いられこれらの鍵は暗号化されあるいは暗号化されないで放送によって供給される。本発明は、データベースシステムの不正利用の防止、著作権の管理、ペーパービューシステム、ビデオオンデマンドシステムにおいて有効であり、さらには電子データ情報システムを利用した電子マーケットの実現において有効な手段である。



【特許請求の範囲】

【請求項1】 放送局、データベース、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって、前記暗号鍵システムは、前記データベースと前記放送局との間は専用回線等のオンライン通信手段あるいはフレキシブルディスク等のオフライン手段で接続され；前記データベースと前記データ通信装置の間は通信回線で接続され；前記放送局と前記受信装置の間は電波で接続され；前記受信装置と前記ユーザ端末装置との間及び前記データ通信装置と前記ユーザ端末装置との間は直接にオンライン手段あるいはフレキシブルディスク等のオフライン手段で接続され；前記データベースは公開鍵と専用鍵を用意して前記放送局に前記公開鍵を供給し；前記放送局は受け取った前記公開鍵を放送し；前記受信装置は受信した前記公開鍵を前記ユーザ端末装置に転送し；前記ユーザ端末装置は転送された前記公開鍵を保存し；ユーザは希望するデータの利用を申し込む際にユーザの秘密鍵を前記受信した公開鍵を用いて暗号化して前記データベースに送信し；データの利用申込を受けた前記データベースは、前記ユーザの前記秘密鍵を前記専用鍵を用いて復号化し、復号された前記ユーザの前記秘密鍵を用いてデータを暗号化し、前記通信回線を経由して前記データ通信装置に送信し；前記ユーザは受け取ったデータを前記ユーザ端末装置に転送し、前記秘密鍵を用いてデータを復号化する暗号鍵システム。

【請求項2】 前記公開鍵に前記データベースのデジタル署名がなされているクレーム1の暗号鍵システム。

【請求項3】 C A T V放送局、課金センタ、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって、前記暗号鍵システムは、前記C A T V放送局と前記受信装置の間及び前記C A T V放送局と前記データ通信装置の間はC A T V回線で接続され；前記受信装置と前記ユーザ端末装置との間及び前記データ通信装置と前記ユーザ端末装置との間は直接にオンライン手段によってあるいはフレキシブルディスク等のオフライン手段で接続され；ユーザはユーザの公開鍵をC A T V放送局に予め登録するか又は利用申込時に提示し；前記C A T V放送局はテレビジョン番組をC A T V放送局の前記秘密鍵を用いて暗号化し、利用申込を行った前記ユーザの公開鍵を用いて前記C A T V放送局の利用許可鍵である秘密鍵を暗号化してC A T V回線を経由して放送し；前記ユーザは前記受信装置で前記テレビジョン番組及び前記秘密鍵を受信し、前記公開鍵に対応する専用鍵を用いて前記秘密鍵を復号化し、復号された前記秘密鍵でテレビジョン番組を復号化する暗号鍵システム。

【請求項4】 C A T V放送局、データ管理センタ、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって、前記暗号鍵システムは、

前記C A T V放送局と前記データ管理センタの間は専用回線等のオンライン通信手段あるいはフレキシブルディスク等のオフライン手段で接続され；前記C A T V放送局と前記受信装置の間及び前記C A T V放送局と前記データ通信装置の間はC A T V回線で接続され；前記受信装置と前記ユーザ端末装置との間及び前記データ通信装置と前記ユーザ端末装置との間は直接にオンライン手段あるいはフレキシブルディスク等のオフライン手段で接続され；前記データ管理センタは公開鍵と供給するデータ各々の秘密鍵を用意し前記C A T V放送局に供給し；前記C A T V放送局は前記データ管理センタの公開鍵を用いて前記データ管理センタの秘密鍵を暗号化して放送し；ユーザは前記データ通信装置を用いて前記C A T V回線を経由し前記C A T V放送局を介して前記データ管理センタにデータの利用を申し込むとともに前記ユーザの公開鍵を送信し；前記データ管理センタは前記データ各々の秘密鍵を用いて各々のデータを暗号化し、前記ユーザの公開鍵を用いて前記データ管理センタの公開鍵を暗号化し、暗号化された各々のデータ、暗号化された前記データ管理センタの公開鍵及びデータ管理センタの専用鍵を前記ユーザに送信し；前記ユーザは前記ユーザの専用鍵を用いて前記データ管理センタの公開鍵を復号化し、復号化された前記データ管理センタの公開鍵を用いて暗号化された前記データ各々の秘密鍵を復号化し、複合化された前記データ各々の秘密鍵を用いて前記各々のデータを復号化する暗号鍵システム。

【請求項5】 前記公開鍵に前記データ管理センタのデジタル署名がなされているクレーム4の暗号鍵システム。

【請求項6】 C A T V放送局、データ管理センタ、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって、前記暗号鍵システムは、ユーザの公開鍵を予め前記データ管理センタに登録しておき；前記データ管理センタは、前記データ管理センタの公開鍵を前記各ユーザの公開鍵を用いて暗号化し、前記データ管理センタの専用鍵を用いて前記データ管理センタの公開鍵にデジタル署名を行い；暗号化された前記データ管理センタの公開鍵及び前記データ管理センタのデジタル署名をC A T V放送局に送信し；前記C A T V放送局は暗号化された前記データ管理センタの公開鍵及びデジタル署名を放送し；前記ユーザは前記ユーザの公開鍵を用いて受信した前記データ管理センタの暗号化公開鍵を復号化するとともに前記復号化されたデータ管理センタの公開鍵を用いてデジタル署名を確認する暗号鍵システム。

【請求項7】 さらに、各ユーザの暗号化されていないユーザ識別情報が暗号化された前記データ管理センタの公開鍵に付与して放送されるクレーム6の暗号鍵システム。

【請求項8】 C A T V放送局、データ管理センタ、受

信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって：前記暗号鍵システムは、ユーザは前記データ管理センタにデータの利用を要求する毎に前記ユーザの公開鍵を前記データ管理センタに提示し；前記ユーザからのデータ利用要求を受けた前記データ管理センタは利用要求されたデータを前記ユーザの公開鍵を用いて暗号化して前記CATV放送局に送信し；前記CATV放送局は受け取った前記暗号化されたデータを放送し；放送された前記暗号化データを受信した前記ユーザは前記暗号化データを前記ユーザの専用鍵を用いて復号化する暗号鍵システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、テレビジョンシステム、データベースシステムあるいは電子情報交換（Electronic Data Interchange：EDI）を利用する商取引システム等において用いられる暗号鍵システムに係るものである。

【0002】

【従来の技術】情報化時代と言われる今日、通常の地上波放送の他に放送衛星（BS）、通信衛星（CS）と呼ばれる衛星放送、同軸ケーブルあるいは光ケーブルを利用したCATVと呼ばれる有線TV放送が普及しつつある。

【0003】同時に数10チャンネルを配信することが出来る衛星放送あるいはCATV放送においては、包括的な契約によって視聴することが出来るスクランブルがかけられていない一般的なチャンネルの他に、包括的な契約によつては視聴することができないスクランブルされた映画・スポーツ・音楽等専門的なチャンネルが設けられている。これらのチャンネルを視聴するためにはスクランブルを解除するするために契約を行う必要があるが、この契約期間は通常1カ月程度の単位で行われるため、随時の契約によって視聴することができない。

【0004】本発明者らは、特開平6-46419号及び特開平6-141004号で公衆電信電話回線を通じて課金センタから視聴許可鍵を入手するとともに課金が行われ、視聴許可鍵を用いて番組毎に異なるスクランブルパターンで行われたスクランブルを解除して番組を視聴するシステムを、特開平6-132916号でそのための装置を提案した。

【0005】これらのシステム及び装置において、スクランブルされた番組利用希望者は通信装置を使用し通信回線を経由して課金センタに利用申し込みを行い、課金センタはこの利用申し込みに対して通信装置に許可鍵を送信するとともに課金処理を行い料金を徴収する。通信装置で許可鍵を受信した利用希望者は通信装置と受信装置を接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によつ

て番組のスクランブルを解除し、利用希望者が番組を利用する。

【0006】特開平6-132916号にはこれらのシステム及び装置の応用として、各々異なるスクランブルパターンでスクランブルされた複数のデータが記録されたテープあるいはディスクを販売あるいは貸与し、ICカード等により利用許可鍵を供給して特定のデータを利用するシステム及び装置も記載されている。

【0007】また、情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータをLAN（Local Area Network）、WAN（Wide Area Network）、これらを相互に接続したインターネットシステムによってコンピュータ通信ネットワークを構成し、相互に利用するデータベースシステムが普及しつつある。

【0008】一方、デジタル化すると情報量が膨大になるためデジタル化することができなかったテレビジョン動画信号を、圧縮することにより情報量を減少させ、実用的なデジタル化を可能にする技術が開発され、これまでにテレビジョン会議用のH.261規格、静止画像用のJPEG（Joint Photographic image coding Experts Group）規格、画像番組用のMPEG1（Moving Picture image coding Experts Group 1）規格及び現在のテレビジョン放送から高精度テレビジョン放送に対応するMPEG2規格が作成された。

【0009】これらの画像圧縮技術を利用したデジタル化技術はテレビジョン放送あるいはビデオ画像記録用に用いられるだけでなく、コンピュータでこれまで扱うことができなかったテレビジョン動画データを扱うことができるようになり、コンピュータが扱う各種のデータとデジタル化されたテレビジョン動画データを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。このマルチメディアシステムもデータ通信に組み入れられ、データベース上のデータの一つとして利用される。

【0010】このようにしてデータベースの利用範囲が拡大する中で、データベース上のデータ利用に対する課金をどのようにして行うかということ及びデータの直接的な利用以外の複製あるいは転送等によって発生する著作権の問題及びデータの加工によって発生する二次的著作権の問題をどのようにして処理するかということが大きな問題となる。課金及び著作権の処理を確実に行うには、正規の利用者でなければデータの利用が不可能であるようにする必要があり、データを暗号化しておくことがそのための最良の手段である。

【0011】また、これまで紙に記載して行ってきた各種取引における情報を電子データ化し、データ通信技術を利用して相互に送受信する電子情報交換（EDI）を利用して電子商取引を行う電子マーケットシステムが検討されており、さらに進んで電子商取引システムの決済

を電子決済で行うことも検討されている。商取引においては取引内容の信頼性が要求され、決済においては安全性が要求される。したがって、このような信頼性と安全性が要求される電子商取引システム及び電子決済システムにおいては、データの改竄あるいは盗用が行われないようにデータを暗号化する必要がある。

【0012】これらのテレビジョンシステム、データベースシステムあるいは電子商取引システム等において、データを暗号化し、暗号化されたデータを復号化して利用するためには暗号鍵が必要であり、データ利用者に対して暗号鍵を渡さなければならないが、この作業は安全性及び確実性が要求されるため非常に煩雑である。

【0013】本発明はその構成においてデータ暗号技術が重要な役割を果たすが、初めにデータ暗号技術について一般的な説明を行う。データ暗号技術においては、平文データMを暗号鍵Kを用いて暗号化し暗号文データCを得る場合を

$$C = E(K, M)$$

と表現し、暗号文データCを暗号鍵Kを用いて復号化し平文データMを得る場合を

$$M = D(K, C)$$

と表現する。

【0014】データ暗号化技術において用いられる代表的な方式として、秘密鍵暗号方式と、公開鍵暗号方式がある。秘密鍵方式は、暗号化と復号化に同じ秘密鍵Ksを使用する暗号方式である。

$$Cmks = E(Ks, M)$$

$$M = D(Ks, Cmks)$$

【0015】公開鍵方式は、暗号鍵として暗号化用の鍵と復号化用の鍵が使用され、暗号化用の鍵が公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵Kbと呼ばれ、復号化用の鍵は専用鍵Kvと呼ばれる。この暗号方式を使用するには、情報を送る側は平文データMをデータを受ける側の公開鍵Kbを用いて暗号化し、

$$Cmkb = E(Kb, M)$$

データを受け取った側は専用鍵Kvを用いて復号化し、

$$M = D(Kv, Cmkb)$$

平文データMを得る。

この公開鍵方式は、暗号の解読が非常に困難である。

【0016】データ暗号技術の応用として、データの信頼性を確保するために電子データ認証手段としてデジタル署名が行われることがある。デジタル署名には、秘密鍵を用いるものと公開鍵を用いるものがあるが、一般的には公開鍵を用いて署名が行われる。公開鍵を用いて行われるデジタル署名において、署名者は文書Mをハッシュ(Hash)アルゴリズムで圧縮した文書mを署名者の専用鍵Kvを用いて暗号化することによりデジタル署名を得、

$$Smkv = E(Kv, m)$$

原文書Mあるいは圧縮文書mとデジタル署名Smkvとを受信者に送信する。受信者は署名者の公開鍵Kbを用いてデジタル署名Smkvを復号化し、

$$m' = D(Kb, Smkv)$$

$m' = m$ であれば、署名が正しいことが確認される。

【0017】これらの暗号鍵を利用者に渡す方法として本発明者らは先願である特願平6-70643号において「暗号鍵システム」と題する発明を提案した。一般的に行われている暗号鍵システムにおいて暗号鍵が利用者だけに渡されるのに対して、この先願発明の暗号鍵システムにおける暗号鍵は利用者以外にも渡される。

【0018】図1に示されたのは特願平6-70643号で提案された暗号鍵システムの構成である。このシステムは、BS・CS・地上波テレビジョンあるいはFM等多重化放送あるいはデータ放送を行う放送局1、データベース2、課金センタ3、受信装置4、データ通信装置5及びユーザ端末装置8から構成されている。放送局1とデータベース2の間及びデータベース2と課金センタ3の間は専用回線等の通信回線あるいはフレキシブルディスク等の手段により接続されている。データベース2とデータ通信装置5の間は公衆回線あるいはCATV回線等の通信回線7で接続されている。放送局1と受信装置4の間は放送電波6で接続されている。受信装置4とユーザ端末装置8との間及びデータ通信装置5とユーザ端末装置8との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。なお、この図において実際で示されたのは暗号化されていない情報の経路であり、破線で示されたのは暗号化されたデータの経路である。

【0019】このシステムにおいて、データベース2はデータ毎に異なる暗号鍵Kdを含む利用許可鍵Kp(以下「許可鍵」という)を放送局1に予め供給する。なお、理解しやすくするために、許可鍵Kpは暗号鍵Kdだけから構成されているものとして説明する。暗号鍵Kdは暗号化されずに供給される場合と共通暗号鍵K0を用いて暗号化され、

$$Ckd0 = E(K0, Kd)$$

暗号化暗号鍵Ckd0として供給される場合がある。暗号鍵Kdが暗号化されて供給される場合には、暗号化暗号鍵Ckd0を復号化するための共通暗号鍵K0がユーザに供給される。この共通暗号鍵K0の供給はユーザがデータベースに登録を行ったときに行われる場合と、暗号化データCmkdが送られるときに暗号化データCmkdとともにユーザに渡される場合がある。

【0020】(a)暗号鍵が暗号化されていない場合。この暗号鍵システムにおいて、放送局1はデータベース2から供給された暗号鍵Kdを電波6を利用して放送する。受信装置4は受信した暗号鍵Kdをユーザ端末装置8に供給し、ユーザ端末装置8は受け取った暗号鍵Kdを半導体メモリ、フレキシブルディスクあるいはハード

ディスク等の記録媒体に保存する。データ利用希望者（ユーザ）はデータ通信装置 5 を用いて通信回線 7 を経由してデータベース 2 にデータ M の利用を申し込む。データ M の利用申し込みを受けたデータベース 2 は利用希望があったデータ M を許可鍵 Kp である暗号鍵 Kd を用いて暗号化し、

$$Cmkd = E(Kd, M)$$

暗号化データ Cmkd を通信回線 7 を経由してユーザのデータ通信装置 5 に送信するとともに課金センタ 3 との間で課金処理を行う。データ通信装置 5 は受け取った暗号化データ Cmkd をユーザ端末装置 8 に供給し、ユーザ端末装置 8 は記録媒体に保存されていた暗号鍵 Kd を用いて暗号化データ Cmkd を復号化する。

$$M = D(Kd, Cmkd)$$

【0021】(b) 暗号鍵が暗号化され、共通暗号鍵が予めユーザに配布されている場合。

この暗号鍵システムにおいて、ユーザがデータベースを利用することを登録するときに、共通暗号鍵 K0 が ROM あるいはフレキシブルディスク等の記録媒体によってユーザに供給され、供給された共通暗号鍵 K0 はユーザ端末装置 8 に保存されている。データベース 2 は暗号鍵 Kd を共通暗号鍵 K0 を用いて暗号化し、

$$Ckdk0 = E(K0, Kd)$$

暗号化暗号鍵 Ckdk0 を放送局 1 に供給する。放送局 1 はデータベース 2 から供給された暗号化暗号鍵 Ckdk0 を電波 6 を利用して放送する。受信装置 4 は受信した暗号化暗号鍵 Ckdk0 をユーザ端末装置 8 に供給し、ユーザ端末装置 8 は初めに暗号化暗号鍵 Ckdk0 を予め保存されている共通暗号鍵 K0 を用いて復号化し、

$$Kd = D(K0, Ckdk0)$$

復号された暗号鍵 Kd を半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存する。

【0022】データ利用希望者はデータ通信装置 5 を用いて通信回線 7 を経由してデータベース 2 にデータ M の利用を申し込む。データの利用申し込みを受けたデータベース 2 は利用希望があったデータ M を暗号鍵 Kd を用いて暗号化し、

$$Cmkd = E(Kd, M)$$

通信回線 7 を経由してデータ通信装置 5 に送信するとともに課金センタ 3 との間で課金処理を行う。データ通信装置 5 は受信した暗号化データ Cmkd をユーザ端末装置 8 に供給し、ユーザ端末装置 8 は保存されていた暗号鍵 Kd を用いて暗号化データ Cmkd を復号化する。

$$M = D(Kd, Cmkd)$$

【0023】(c) 暗号鍵が暗号化されており、共通暗号鍵が暗号化データとともにユーザに配布される場合。この暗号鍵システムにおいて、データベース 2 は共通暗号鍵 K0 を用いて暗号鍵 Kd を暗号化し、

$$Ckdk0 = E(K0, Kd)$$

放送局 1 に供給する。放送局 1 はデータベース 2 から供給された暗号化暗号鍵 Ckdk0 を電波 6 を利用して放送する。受信装置 4 は受信した暗号化暗号鍵 Ckdk0 をユーザ端末装置 8 に供給し、ユーザ端末装置 8 は暗号化暗号鍵 Ckdk0 を半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存しておく。

【0024】データ利用希望者はデータ通信装置 5 を用いて通信回線 7 を経由してデータベース 2 にデータ M の利用を申し込む。データの利用申し込みを受けたデータベース 2 は利用希望があったデータ M を暗号鍵 Kd を用いて暗号化し、

$$Cmkd = E(Kd, M)$$

共通暗号鍵 K0 と一緒に通信回線 7 を経由してデータ通信装置 5 に送信するとともに課金センタ 3 との間で課金処理を行う。データ通信装置 5 は受信した暗号化データ Cmkd と共通暗号鍵 K0 をユーザ端末装置 8 に供給し、ユーザ端末装置 8 は共通暗号鍵 K0 を用いて記録媒体に保存されていた暗号化暗号鍵 Ckdk0 を復号化し、

$$Kd = D(K0, Ckdk0)$$

復号化された暗号鍵 Kd を用いて暗号化データ Cmkd を復号化する。

$$M = D(Kd, Cmkd)$$

【0025】

【発明の概要】本願においては、この先願に記載された暗号鍵システムの発明をテレビジョンシステム、データベースシステムあるいは電子商取引システム等に適用するための具体的な構成を提供する。このシステムは放送局、データベース、受信装置、データ通信装置及びユーザ端末装置から構成され、暗号鍵方式としては秘密鍵方式、公開鍵方式が採用され、さらにデジタル署名が用いられ、このとき用いられる暗号鍵は暗号化されるあるいは暗号化されないで放送によって供給される。本発明は、データベースシステム、ペーパービューシステム、ビデオオンデマンドシステムにおける不正利用の防止、著作権の管理において有効であり、さらには電子情報情報システムを利用した電子マーケットの実現において有効な手段である。

【0026】

【実施例】以下、図 2～図 4 を用いて本願発明の実施例を説明する。

【第 1 実施例】図 2 に示されたのは本願発明をデータベースシステムに適用した第 1 実施例の暗号鍵システムであり、このシステムは、BS・CS・地上波テレビジョンあるいは FM 放送等による多重化放送あるいはデジタル放送によりデータ放送を行う放送局 11、動画データを含む種々のデータが蓄積されたデータベース 12、課金センタ 13、放送局 11 が放送するデータ放送を受信する受信装置 14、データベース 12 と通信を行うデータ通信装置 15 及びデータを利用するユーザ端末装置 18 から構成されている。

【0027】データベース12と放送局11との間及びデータベース12と課金センタ13の間は専用回線等の通信回線で接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。データベース12とデータ通信装置15の間は公衆回線あるいはCATV回線等の通信回線17で接続されている。放送局11と受信装置14の間は地上波テレビジョン放送、衛星テレビジョン放送、CATV放送、FM放送あるいは衛星データ放送等の電波16で接続されている。受信装置14とユーザ端末装置18との間及びデータ通信装置15とユーザ端末装置18との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。この図において実線で示されたのは暗号化されていないデータの経路であり、破線で示されたのは暗号化されたデータの経路である。なお、データベース12と放送局11との間及びデータベース12と課金センタ13の間のデータの受け渡しは原則として専用回線あるいはフレキシブルディスクにより行われるが、この他に公衆回線あるいは放送衛星、通信衛星、地上波放送によって行うこともできる。その場合にデータは暗号化される。

【0028】このシステムにおいては、暗号鍵方式として秘密鍵方式と公開鍵方式が採用される。データベース12は公開鍵Kbdと専用鍵Kvdを用意し、放送局11に公開鍵Kbdを供給する。公開鍵Kbdを受け取った放送局11はアナログテレビジョン映像信号の繰繰消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、FM多重データ放送あるいはデジタルデータ放送で公開鍵Kbdを放送する。なお、この場合公開鍵Kbdにデータベース11のデジタル署名を行うようにすることもできる。

【0029】このときにデータ利用の便のため、利用することができるデータのタイトルを記載した目次、データの内容紹介、商品カタログ、発注書、無記載の小切手、著作権情報を暗号化することなく供給することもある。放送された公開鍵Kbdを受信した受信装置14は、公開鍵Kbdをユーザ端末装置11に転送し、転送された公開鍵Kbdを受け取ったユーザ端末装置18は半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に公開鍵Kbdを保存する。

【0030】目次あるいは内容紹介等によって利用を希望するデータを選択したユーザは、データ通信装置15を用いて通信回線17を経由してデータベース12にデータMの利用を申し込む。このときユーザは自分の秘密鍵Kksuを受信したデータベース12の公開鍵Kbdを用いて暗号化し、 $Cksukbd = E(Kbd, Mksu)$

データベース12に送信する。

【0031】データベース12は、暗号化されたユーザの秘密鍵Cksukbdを専用鍵Kvdを用いて復号化し、

$Ksu = D(Kvd, Cksukbd)$

利用申し込みがなされたデータMを復号化されたユーザの秘密鍵Ksuを用いて暗号化し、

$Cmksu = E(Ksu, M)$

通信回線17を経由してユーザのデータ通信装置15に送信する。

【0032】自分の秘密鍵Ksuを用いて暗号化されたデータCmksuを受け取ったユーザはユーザ端末装置18で、自分の秘密鍵Ksuを用いて暗号化された暗号化データCmksuを復号化し、

$M = D(Ksu, Cmksu)$

利用する。

【0033】このシステムにはデータベース12に連動する課金センタ13が設けられている。この課金センタ13は、データが有料で提供される場合には利用されるが、データがショッピング情報等無料で提供されるデータである場合には利用されない。しかし、ショッピング情報等無料で提供されるデータであっても、受・発注にともなう代金清算が行われる場合には利用される。

【0034】【第2実施例】図3に示されたのは、本願発明を利用希望者からの希望に応じてテレビジョン番組を放送するビデオオンデマンド（Video On Demand: VOD）システムに適用した第2実施例の暗号鍵システムである。このシステムはCATV放送局21、課金センタ23、受信装置24、データ通信装置25及びユーザ端末装置28から構成される。課金センタ23は、テレビジョン番組が有料で提供される場合には利用されるが、テレビジョン番組が広告付き等無料で提供される場合には利用されない。このシステムにおいて、暗号化されたテレビジョン放送番組と暗号鍵とは単一の経路であるCATV回線27で送信される。

【0035】CATV放送局21と課金センタ23の間は専用回線等の通信回線により電氣的に接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。CATV放送局21と受信装置24の間及びCATV放送局21とデータ通信装置25の間はCATV回線27で接続されている。受信装置24とユーザ端末装置28との間及びデータ通信装置25とユーザ端末装置28との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。この図において実線で示されたのは暗号化されていないデータの経路であり、破線で示されたのは暗号化されたデータの経路である。なお、CATV放送局21と課金センタ23の間のデータの受け渡しは原則として専用回線あるいはフレキシブルディスクにより行われるが、この他に公衆回線あるいは放送衛星、通信衛星、地上波放送によって行うこともできる。その場合にデータは暗号化される。

【0036】このシステムにおいては、CATVシステムもデータベースの一種として扱われ、暗号鍵方式とし

て秘密鍵方式と公開鍵方式が採用される。このVODシステムを利用するユーザは自分の公開鍵KbuをCATV放送局21に予め登録しておくあるいは利用申込時に通信装置25を用いて送信する。

【0037】CATV放送局21は送信されたユーザの公開鍵Kbuを用いてCATV放送局21の秘密鍵Ksbを暗号化し、

$Cksbku = E(Kbu, Ksb)$

CATV回線27を経由してデータ通信装置25に送信する。一方、テレビジョン番組MはCATV放送局21の秘密鍵Ksbを用いて暗号化され、

$Cmksb = E(Ksb, M)$

CATV回線27を経由して受信装置24に放送される。

【0038】ユーザは受信したCATV放送局21の暗号化秘密鍵Cksbkuをユーザの専用鍵Kvuを用いて復号化し、

$Ksb = D(Kvu, Cksbku)$

復号されたCATV放送局21の秘密鍵Ksbを用いて暗号化テレビジョン番組Cmksbを復号化し、

$M = D(Ksb, Cmksb)$

利用する。

【0039】また、この暗号鍵システムは暗号化が可能ならばCATV以外のテレビジョン放送、音声放送あるいはデータ放送に対しても適用可能である。また、放送局から暗号鍵を送信する方法として、アナログテレビジョン映像信号の掃線消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、FM多重データ放送あるいはデジタルデータ放送が利用可能である。

【0040】さらに、この暗号鍵システムは本発明者らが提案した先願である特願平6-64889号、特願平6-237673号、特願平6-264199号、特願平6-264201号、特願平6-269959号に記載されたデータ著作権管理システムにおいて暗号鍵を配布する場合にも利用可能である。また、この暗号鍵システムは特開平6-132916号公報に記載されている本発明者らが提案した、複数の情報が複数の異なるパターンで暗号化されて記録されているCD-ROM等の記録媒体を利用する場合にも適用可能である。これらの先願発明について説明する。

【0041】特願平6-64889号に記載されているデータ著作権管理システムの概要は次のようなものである。デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示（音声化を含む）、管理、複写、加工、転送における著作権の管理を行うために、利用申し込み者に対して暗号化されたデータの利用を許可する鍵の他に、必要に応じて著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を送信する。著

作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0042】著作権管理プログラム、著作権情報及び著作権管理メッセージは、各許可鍵とともに全体が供給される場合、データとともに全体が供給される場合及び一部が許可鍵とともに供給され、一部がデータとともに供給される場合がある。データ、許可鍵、著作権管理メッセージ、著作権情報及び著作権管理プログラムには、暗号化された状態で送信されるが利用時には暗号が解かれる場合、暗号化された状態で送信され表示の際のみに暗号が解かれその他の場合は暗号化された状態である場合、全く暗号化されない場合、の3つの場合がある。

【0043】特願平6-237673号に記載されているデータ著作権管理システムの概要は次のようなものである。このデータベース著作権管理システムは、暗号化されていないデータが蓄積されたデータベース、データベースからの暗号化されたデータを放送する衛星放送局等の放送局あるいはデータベースの暗号化されたデータが記録されたCD-ROM等の記録媒体であるデータ供給手段、通信ネットワーク、暗号鍵を管理する鍵管理センタ、データベースの著作権を管理する著作権管理センタから構成され、データベースを利用するためのデータベース利用プログラムおよび著作権を管理するための著作権管理プログラム、第1の暗号鍵、第2の暗号鍵が使用される。

【0044】1次ユーザはデータベースを利用するために予め鍵管理センタに登録を行い、その際にデータベース利用プログラムを配布されている。このデータベース利用プログラムには、1次ユーザに関する情報および情報を利用して所定のアルゴリズムにより1次ユーザ固有の暗号鍵を生成するプログラムが含まれている。データは暗号化されずにデータベースに蓄積されており、放送され、記録媒体に記録されあるいは通信ネットワークを経由することによって配布されるときに第1の暗号鍵で暗号化され、暗号化データとされる。暗号化データは、放送あるいは通信ネットワークを経由して配布された場合には1次ユーザ端末装置の半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存され、CD-ROM記録媒体に記録されて配布された場合にはそのままの状態あるいは1次ユーザ端末装置の半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存される。

【0045】データベースから直接にデータを利用する1次ユーザは通信ネットワークを経由して、鍵管理センタに暗号化データを復号化して利用するための鍵を要求するが、このときに1次ユーザに関する情報を提示する。鍵管理センタは1次ユーザに関する情報を著作権管

理センタに転送し、著作権管理センタは 1 次ユーザに関する情報 I を利用して所定のアルゴリズムにより 1 次ユーザ固有の暗号鍵を生成し、生成された 1 次ユーザ暗号鍵を利用して著作権管理プログラム、第 1 の暗号鍵および第 2 の暗号鍵を暗号化して、鍵管理センタに転送する。この 1 次ユーザに関する情報を利用して生成された暗号鍵を用いて暗号化された著作権管理プログラムは 1 次ユーザに固有のものである。

【0046】暗号化された著作権管理プログラムを受け取った鍵管理センタは各々暗号化された著作権管理プログラム、第 1 の暗号鍵、第 2 の暗号鍵を 1 次ユーザ端末装置に対して通信ネットワークを経由して 1 次ユーザ端末装置に送信し、1 次ユーザは受信した暗号化著作権管理プログラム、暗号化第 1 暗号鍵、暗号化第 2 暗号鍵を半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存する。

【0047】1 次ユーザは、予め配布されているデータベース利用プログラムを用いて所定のアルゴリズムにより 1 次ユーザに関する情報を利用して 1 次ユーザ固有の暗号鍵を生成し、生成された暗号鍵を用いて暗号化著作権管理プログラム、暗号化第 1 暗号鍵および暗号化第 2 暗号鍵を復号化し、復号された第 1 の暗号鍵を用いて暗号化データを復号化する。

【0048】以後復号されたデータの保存、コピーあるいは転送を行う場合には復号された著作権管理プログラムにより復号された第 2 暗号鍵を用いて暗号化が行われ、暗号化データが 1 次ユーザ端末装置内の半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存され、1 次ユーザが保存された暗号化データを利用するときは第 2 暗号鍵を用いて復号化し、この操作が繰り返されて 1 次利用が行われる。

【0049】暗号化データが外部記憶媒体にコピーされたときあるいは通信ネットワークを経由して 2 次ユーザ端末装置に転送された場合には、著作権管理プログラムにより第 1 暗号鍵および第 2 暗号鍵が廃棄され、1 次ユーザは暗号化データを利用することができなくなる。このとき、暗号化データが 1 次ユーザ端末装置に保存されている場合には、保存されている暗号化データに、1 次ユーザについての暗号化されていない情報が付加される。

【0050】1 次ユーザが再度暗号化データを利用する場合には、著作権管理センタから第 1 暗号鍵と第 2 暗号鍵の再交付を受け、この再交付が行われたことにより、この 1 次ユーザから暗号化データのコピーあるいは転送を受けた 2 次ユーザが存在することが確認され、2 次ユーザの存在が著作権管理センタに記録される。

【0051】コピーあるいは転送された暗号化データを受け取った 2 次ユーザは著作権管理センタに暗号化データの 2 次利用を申込む。2 次ユーザは 1 次ユーザと異なり予め鍵管理センタに登録をしておく必要はなく、利用

申込時に暗号化データのコピーあるいは転送を受けた 1 次ユーザの情報を著作権管理センタに提示することにより利用申込が受理される。このときに 1 次ユーザ情報が提示されない場合には、そのユーザは 1 次ユーザから暗号化データのコピーあるいは転送を受けた 2 次ユーザではなく、1 次ユーザであると認められるため、その 2 次利用申込は受理されない。2 次利用申込を受理した著作権管理センタは暗号化データを復号化するための第 2 暗号鍵、復号された暗号化データを再暗号化および再復号化するための第 3 暗号鍵、これらの復号化、再暗号化、再復号化を行う著作権管理プログラムを 2 次ユーザに送信する。

【0052】特願平 6-264199 号に記載されている著作権管理システムの概要は次のようなものである。この著作権管理システムにおいては、ユーザが用意する第 1 の公開鍵、第 1 の公開鍵に対応する第 1 の専用鍵、第 2 の公開鍵、第 2 の公開鍵に対応する第 2 の専用鍵とデータベース側が用意する第 1 の秘密鍵及び第 2 の秘密鍵が使用される。

【0053】データベース側では、暗号化されていないデータを第 1 の秘密鍵を用いて暗号化し、第 1 の秘密鍵を第 1 の公開鍵を用いて暗号化するとともに第 2 の秘密鍵を第 2 の公開鍵を用いて暗号化し、これらの暗号化されたデータ、暗号化第 1 秘密鍵及び暗号化第 2 秘密鍵をユーザに送信する。

【0054】ユーザは、暗号化第 1 秘密鍵を第 1 専用鍵を用いて復号化し、復号化された第 1 秘密鍵を用いて暗号化データを復号化し、利用するとともに、暗号化された第 2 秘密鍵を第 2 専用鍵を用いて復号化し、復号化第 2 秘密鍵は復号化以降におけるデータの保存・複写・転送時の暗号鍵として使用される。

【0055】特願平 6-264201 号に記載されているデータ著作権管理システムの概要は次のようなものである。データベースから入手した複数の暗号化されたデータを加工することにより新しいデータを作成し、暗号化して他人に供給する場合に、原材料である複数のデータの暗号鍵と、加工プロセスである加工プログラムをデジタル署名化したデータを利用許可鍵として使用する。加工された暗号化されたデータを受け取ったユーザが著作権管理センタにデジタル署名を提示して利用申込を行うと、著作権管理センタはデジタル署名に基づいて加工者を確認し、加工者が被加工データの正当なユーザであることが確認された場合にのみ、利用申込者に対して利用のための暗号鍵を提供する。

【0056】特願平 6-269959 号に記載されている方法の概要は次のようなものである。1 次ユーザはデータベースから原データが第 1 の暗号鍵で暗号化された暗号化データを受け取り、復号化して利用するが、その後は第 1 の暗号鍵、1 次ユーザデータ、データ利用回数の中の 1 つあるいはこれらを組み合わせで所定のアルゴ

リズムにより生成された第2の暗号鍵で暗号化されて保存、複写、転送が行われる。2次ユーザがデータの2次利用を要求すると著作権管理センタは原データの第1の暗号鍵、1次ユーザデータ、データ利用回数内の1つあるいはこれらを組み合わせて所定のアルゴリズムにより第2の暗号鍵を生成し2次ユーザに提供する。第2の暗号鍵を提供された2次ユーザは、第2の暗号鍵を用いて暗号化された原データを復号化し、利用する。

【0057】[第3実施例] 図4に示されたのは本願発明をデータベースシステムあるいはVODシステムに適用した第3実施例の暗号鍵システムである。この暗号鍵システムも図3に示された第2実施例の暗号鍵システムと同様に暗号鍵とテレビジョン放送番組とはCATV回線である単一の経路を通るが、これらを見る経路を通るようにすることが可能であることももちろんのことである。このシステムはデータ放送を行うCATV放送局31、データベースあるいはビデオシステム等のデータ管理センタ33、受信装置34、データ通信装置35及びユーザ端末装置38から構成される。

【0058】データ管理センタ33とCATV放送局31の間は専用回線等の通信回線で接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。CATV放送局31と受信装置34の間及びCATV放送局31とデータ通信装置35の間はCATV回線37で接続されている。なお、CATV回線37に代えて他の適当なデータ放送あるいはデータ通信可能な通信回線を使用することが可能である。受信装置34とユーザ端末装置38との間及びデータ通信装置35とユーザ端末装置38との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。この図において実線で示されたのは暗号化されていないデータの経路であり、破線で示されたのは暗号化されたデータの経路である。なお、データ管理センタ33とCATV放送局31の間のデータの受け渡しは原則として専用回線あるいはフレキシブルディスクにより行われるが、この他に公衆回線あるいは放送衛星、通信衛星、地上波放送によって行うこともできる。その場合にデータは暗号化される。

【0059】このシステムにおいて採られる暗号鍵方式は秘密鍵方式と公開鍵方式である。データ管理センタ33は供給される全データに共通する公開鍵Kbd及び専用鍵Kvdとデータ各々で異なる秘密鍵Ksdiを用意しCATV放送局31に供給する。CATV放送局31は受け取った秘密鍵Ksdiをデータ管理センタ33の公開鍵Kbを用いて暗号化して、

Cksdikbd = E (Kbd, Ksdi)
アナログテレビジョン映像信号の掃線消去期間中の走査線を利用して文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用してデータ放送、FM多重データ放送あるいはデジタルデータ放送により放送する。こ

のときにデータ利用の便のため、利用することができるデータのタイトルを記載した目次、あるいはデータの利用を促進するため、データの概要を説明する内容紹介を暗号化することなく供給することもできる。

【0060】目次あるいは内容紹介によって利用を希望するデータを選択したユーザは、データ通信装置35を用いてCATV回線37を経由しCATV放送局31を介してデータ管理センタ33にデータの利用を申し込む。このときユーザは自分の公開鍵Kbuをデータ管理センタ33に送信する。ユーザからの利用申し込みを受けたデータ管理センタ33は秘密鍵Ksdiを用いてデータMを暗号化して

Cmksdi = E (Ksdi, M)

ユーザ端末装置38に送信する。その時データ管理センタの専用鍵Kvdが利用申し込みを行ったユーザの公開鍵Kbuを用いて暗号化され、

Ckvdibu = E (Kbu, Kvd)

ユーザ端末装置38に送信される。

【0061】データ管理センタの暗号化専用鍵Ckvdibuを受け取ったユーザは、データ管理センタの暗号化専用鍵Ckvdibuをユーザの専用鍵Kvuを用いて復号化し、

Kvd = D (Kvu, Ckvdibu)

復号化されたデータ管理センタの専用鍵Kvdを用いて暗

号化秘密鍵Cksdikbdを復号化し、

Ksdi = D (Kvd, Cksdikbd)

復号されたデータ管理センタの秘密鍵Ksdiを用いて暗

号化データCmksdiを復号化して

M = D (Ksdi, Cmksdi)

利用する。

【0062】[第4実施例] 第4実施例のシステム構成は図4に示された第3実施例と同じであるから説明は省略する。このシステムにおいて採られる暗号鍵方式は第3実施例と同様に秘密鍵方式と公開鍵方式であるが、第3実施例では利用申し込みを行ったユーザの公開鍵Kbuでデータ管理センタの専用鍵Kvdが暗号化されてユーザに送信されるのに対し、第4実施例においてはデータ管理センタの専用鍵Kvdが予めICカード等を用いて配布されユーザ端末装置内に保存されている点及び第3実施例においてはデータMがデータの利用を申し込みに応じて配信されるのに対し、第4実施例ではデータMがCATV回線あるいは衛星放送により利用希望とは無関係に放送される点で異なる。

【0063】ユーザがデータ管理センタとデータベースを使用する包括的な契約を締結する際に、供給される全データに共通するデータ管理センタの専用鍵KvdがICカード等の記録媒体によりあるいはCATV回線37を経由して予めユーザに配布され、ユーザ端末装置38内の半導体メモリ、ハードディスク装置あるいはフレキシブルディスクに保存されている。データ管理センタ33は公開鍵Kbdと供給されるデータ各々で異なる秘密鍵K

sdiを用意しCATV放送局31に供給する。秘密鍵Ksdiを受け取ったCATV放送局31はその秘密鍵Ksdiを公開鍵Kbdを用いて暗号化し、
 $Cksdikbd = E(Kbd, Ksdi)$
 暗号化秘密鍵Ksdikbdをアナログテレビジョン映像信号の帰線消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、FM多重データ放送あるいはデジタルデータ放送により放送する。このときにデータ利用の便のため、利用することができるデータのタイトルを記載した目次、あるいはデータの利用を促進するため、データの概要を説明する内容紹介を暗号化することなく供給することもできる。

【0064】CATV放送局31は、秘密鍵Ksdiを用いてデータMを暗号化し、
 $Cmksdi = E(Ksdi, M)$
 CATV回線により利用希望とは無関係に一方的に放送する。ユーザは、目次あるいは内容紹介に基づきCATV回線で放送されているデータの中から希望するデータを受信装置34を用いてユーザ端末装置38に取り込む。

【0065】ユーザは予め配布されてユーザ端末装置38内の半導体メモリ、ハードディスク装置あるいはフレキシブルディスクに保存されているデータ管理センタの専用鍵Kvdを用いて暗号化秘密鍵Ksdikbdを復号化し、
 $Ksdi = D(Kvd, Cksdikbd)$
 復号化された秘密鍵Ksdiを用いて暗号化データCmksdiを復号化し、
 $M = D(Ksdi, Cmksdi)$
 利用する。

【0066】暗号鍵を配布するためのその他の変形実施例を説明する。

【第5実施例】これまでに説明した実施例において、データ管理センタの公開鍵Kbdは通信回線経由ではなく放送局から放送されるため、それが真正なものであるか否か確認することができない。そのような場合にはデータ管理センタの公開鍵Kbdにデータ管理センタの専用鍵Kvdを用いてデジタル署名Sskbdkvdを行い、
 $Sskbdkvd = E(Kvd, Kbd)$
 データ管理センタの公開鍵Kbdとともにデジタル署名Sskbdkvdを放送する。ユーザは、受信したデータ管理センタの公開鍵Kbdを用いてデジタル署名Sskbdkvdを確認し、
 $Kbd = D(Kbd, Sskbdkvd)$
 それが真正なものであるれば使用する。

【0067】【第6実施例】第5実施例においてデータ管理センタがデータベースの利用を予め登録する会員制を採用している場合には、さらに会員であるユーザの公開鍵Kbuiを予めデータ管理センタに登録しておく。デ

ータ管理センタは、データ管理センタの公開鍵Kbdを各ユーザの公開鍵Kbuiを用いて暗号化する。
 $Ckdbkui = E(Kbui, Kbd)$
 また、データ管理センタの公開鍵Kbdにデータ管理センタの専用鍵Kvdを用いてデジタル署名Sskbdkvdを行い、
 $Sskbdkvd = E(Kvd, Kbd)$
 ユーザ毎に異なる暗号化公開鍵Ckdbkui及びデジタル署名Sskbdkvdを放送局に送り、放送局は受け取った暗号化公開鍵Ckdbkui及びデジタル署名Sskbdkvdを放送する。このとき、必要ならば各ユーザの暗号化されていないユーザ識別情報を暗号化公開鍵Ckdbkuiに付与して放送する。放送された暗号化公開鍵Ckdbkui及びデジタル署名Sskbdkvdを受け取ったユーザはそのユーザの公開鍵Kvuiを用いてデータ管理センタの暗号化公開鍵Ckdbkuiを復号化し、
 $Kbd = D(Kvui, Ckdbkui)$
 復号化されたデータ管理センタの公開鍵Kbdをユーザの端末装置内に保存しておく。また、ユーザは、受信したデータ管理センタの公開鍵Kbdを用いてデジタル署名Sskbdkvdを確認し、
 $Kbd = D(Kbd, Sskbdkvd)$
 それが真正なものであるれば保存されていたデータ管理センタの公開鍵Kbdを使用する。このようにすると、ユーザ個々に異なる暗号鍵を配布することができる。
 【0068】【第7実施例】ユーザはデータ管理センタにアクセスする毎に又はリクエストする毎に自分の公開鍵Kbuをデータ管理センタに提示する。ユーザからのリクエストを受けたデータ管理センタは要求されたデータMをユーザの公開鍵Kbuを用いて暗号化し、
 $Cmkbu = E(Kbu, M)$
 放送局に送り、放送局は受け取った暗号化データCmkbuを放送する。放送された暗号化データCmkbuを受信したユーザはユーザの専用鍵Kvuを用いて復号化して、
 $M = D(Kvu, Cmkbu)$
 利用する。

【0069】図5を用いて、本願発明の暗号鍵システムを使用した応用例を示す。この図に示された各応用例は電子情報交換システムを利用する電子マーケット取引に、(a)に示されたものは小売店が行うクレジット決済に、(b)に示されたのは電子小切手による決済に、(c)に示されたのはメーカ等が行う卸売販売に、各々これらの暗号鍵システムを適用した場合の構成である。これらのシステムは、秘密鍵方式に加えてデジタル署名が利用され、ユーザ42、インターネット上のWWW(World Wide Web)サーバである小売店43、金融機関44あるいはメーカ等である卸売店45から構成される。

【0070】【第8実施例】(a)に示された小売店におけるクレジット決済において、小売店43は発注書のフォーマット、クレジットカードフォーマット、広告、

カタログ、予告編、製品説明、データベースの紹介や目次/料金表/価格表などのデータMsを衛星41あるいはCATV回線を経由して放送する。発注書フォーマット等のデータMs及び小売店43の公開鍵Kbsを受け取ったユーザ42は、小売店43の公開鍵Kbsを用いてユーザの秘密鍵Ksuを暗号化し、

$$Cksuksb = E(Kbs, Ksu)$$

広告、カタログ、製品説明、料金価格表等の情報に基づいて注文内容、支払金額、クレジットカード番号等の事項Muを発注書にユーザ42の秘密鍵Ksuを用いて暗号化して記入し、

$$Cmksu = E(Ksu, Mu)$$

必要に応じて事項Muを圧縮文書muにしてユーザ42の専用鍵Kvuを用いてデジタル署名を行い、

$$Smukvu = E(Kvu, mu)$$

ユーザ42の公開鍵Kbuを添付してネットワーク47を経由して小売店43に送信する。

【0071】発注書等を受け取った小売店43は、小売店43の専用鍵Kvsを用いてユーザ42の暗号化秘密鍵Cksuksbを復号化し、

$$Ksu = D(Kvs, Cksuksb)$$

復号化されたユーザ42の秘密鍵Ksuを用いて暗号化発注書Cmksuを復号化し、

$$Mu = D(Ksu, Cmksu)$$

受注処理を実行する。さらにユーザ42が添付した公開鍵Kbuを用いてユーザ42のデジタル署名Smukvuを確認し、

$$mu = D(Kbu, Smukvu)$$

ユーザ42にネットワーク47を経由してレシートを返信する。このシステムでは、発注書に記入されるクレジットカード番号を暗号化して送付しているためクレジットカード番号の盗用を防止することができる。

【0072】また、小売店43が発注書フォーマット、クレジットカードフォーマット、広告、カタログ、予告編、製品説明、データベースの紹介や目次/料金表/価格表などのデジタルデータMs1を圧縮文書ms1とし、これに小売店43の専用鍵Kvsを用いてデジタル署名を行い、

$$Sms1kvs = E(Kvs, ms1)$$

小売店43の公開鍵Kbsを添付して放送し、ユーザが小売店43の公開鍵Kbsを用いてデジタル署名Sms1kvsを確認

$$ms' = D(Kbs, Sms1kvs)$$

するようにすることにより、取引がより確実なものとなる。

【0073】【第9実施例】(b)に示された電子小切手による決済において、金融機関44はデジタルデータである無記載小切手フォーマットMfに金融機関44の公開鍵Kbfを添付して衛星41あるいはCATV回線を経由して放送する。無記載小切手フォーマットMfを受

信したユーザ42は、金融機関の公開鍵Kbfを用いてユーザ42の秘密鍵Ksuを暗号化し、

$$Cksukbf = E(Kbf, Ksu)$$

支払先と支払金額についての事項Muをユーザ42の秘密鍵Ksuを用いて暗号化して記入し、

$$Cmksu = E(Ksu, Mu)$$

必要に応じて事項Muを圧縮文書muとし、これにユーザ42の専用鍵Kvuを用いてデジタル署名を行って

$$Smukvu = E(Kvu, mu)$$

ユーザ42の公開鍵Kbuと、金融機関44の公開鍵Kbfで暗号化されたユーザ42の暗号化秘密鍵Cksukbfを添付してネットワーク47を経由して金融機関44に送信する。

【0074】記載済み小切手を受け取った金融機関44は、金融機関の専用鍵Kvfを用いてユーザ42の暗号化秘密鍵Cksukbfを復号化し、

$$Ksu = D(Kvf, Cksukbf)$$

復号化されたユーザの秘密鍵Ksuを用いて支払先と支払金額の暗号化データCmksuを復号化し、

$$Mu = D(Ksu, Cmksu)$$

記載された内容を確認し、為替交換処理を実行する。さらにデジタル署名Smukvuが有るものはユーザ42が添付した公開鍵Kbuを用いてユーザ42を確認し、

$$mu' = D(Kbu, Smukvu)$$

確認書Ms2をユーザ42が添付した公開鍵Kbuを用いて暗号化し、

$$Cms2kbu = E(Kbu, Ms2)$$

ネットワーク47を経由してユーザ42に返信する。

【0075】金融機関44からの暗号化確認書Cms2kbuを受け取ったユーザは、ユーザ42の専用鍵Kvuを用いて暗号化確認書Cms2kbuを復号化して

$$Ms2 = D(Kvu, Cms2kbu)$$

内容を確認する。このシステムによれば、支払先と支払金額を暗号化して小切手に記入しているため小切手に記載された内容の盗用を防止することができる。

【0076】また、デジタルデータである無記載小切手フォーマットMfを圧縮文書mfとし、これに金融機関44の専用鍵Kvfを用いてデジタル署名を行い、

$$Smfkfv = E(Kvf, mf)$$

金融機関44の公開鍵Kbfを添付して放送し、ユーザが金融機関44の公開鍵Kbfを用いてデジタル署名Smkfvを確認

$$mf' = D(Kbf, Smfkfv)$$

するようにし、さらに確認書Msを圧縮文書msとし、これにユーザが添付した公開鍵Kbuを用いてデジタル署名を行う

$$Smskbu = E(Kbu, ms)$$

ようにすることにより、金融機関が記入者を確認することができる。

【0077】【第10実施例】(c)に示されたメーカ

等の卸売店45において、卸売店45は見積依頼書フォーマットMw1を圧縮データmw1としこれに卸売店45の専用鍵Kvwを用いてデジタル署名を行い、

$Smw1kvw = E(Kvw, mw1)$

卸売店45の公開鍵Kbwを添付して衛星41あるいはCATV回線を経由して放送する。放送された見積依頼書フォーマットMw1と卸売店45の公開鍵Kbwを受け取った小売店であるユーザ42は、見積依頼書Muを卸売店45の公開鍵Kbwを用いて暗号化し、

$Cmkwb = E(Kbw, Mu)$

ネットワーク47を経由して卸売店45に送信する。このとき、必要に応じて見積依頼書Muを圧縮データmuとし、これにユーザ42の専用鍵Kvuを用いてデジタル署名を行って、

$Smkvu = E(Kvu, mu)$

ユーザ42の公開鍵Kbuとともに卸売店45に送信する。

【0078】暗号化見積依頼書Cmkwbを受け取った卸売店45は、卸売店45の専用鍵Kvwを用いて暗号化見積依頼書Cmkwbを復号化し、

$Mu = D(Kvw, Cmkwb)$

記載された見積依頼内容Muを確認し、見積作業を実行する。さらにデジタル署名Smkvuがされている場合には送信されたユーザ42の公開鍵Kbuを用いてデジタル署名を確認し、

$mu = D(Kbu, Smkvu)$

見積依頼書を確認する。見積作業を行った卸売店45は、見積書Mw2をユーザ42の公開鍵Kbuを用いて暗号化し、

$Cmw2kbu = D(Kbu, Mw2)$

ネットワーク47を経由してユーザ42に送信する。

【0079】卸売店45の暗号化見積書Cmw2kbuを受け取ったユーザ42は、ユーザ42の専用鍵Kvuを用いて復号化する。

$Mw2 = D(Kvu, Cmw2kbu)$

このシステムによれば、公開鍵と専用鍵を使用しているため、見積書の内容が盗用されるおそれなく、ユーザ毎に異なる見積を行うことができる。

【0080】これら(a)～(c)に示されたシステムにおいては、秘密性を要しない各種フォーマット及び広告とを衛星放送あるいはCATV放送によって放送するため、データの送信を効果的に行うことができる。

【0081】以上説明したように、本発明の暗号化システムを用いることによりこれまで別々にシステムとして存在してきたテレビジョン放送あるいは音声放送等の一般的な情報メディアとコンピュータを用いたデータ通信メディアとを融合したマルチメディアシステムを実現することができる。以下、マルチメディアシステムを実現した具体的な構成を説明する。

【0082】現行のテレビジョン放送は地上波放送、衛

星放送あるいはCATV放送によりアナログ方式で行われ、一方最も一般的なデータ通信回線は電線を利用した公衆回線である。このようなシステム構成においてビデオオンデマンドを実現するシステムとして基本的な構成は図2に示された第1実施例の暗号化システムを利用することができる。放送局はアナログテレビジョン放送番組の垂直帰線期間の走査線あるいは音声帯域の副音声帯域に多重して放送局の公開鍵Kbbを放送する。

【0083】テレビジョン番組利用希望者は自分の秘密鍵Ksuを放送された放送局の公開鍵Kbbを用いて暗号化し、

$Ckskbb = E(Kbb, Ksu)$

暗号化秘密鍵Ckskbbを通信回線を経由して放送局に送信して利用申込を行う。

【0084】放送局は放送局の専用鍵Kvbを用いて利用希望者の暗号化秘密鍵Ckskbbを復号化し、

$Ksu = D(Kvb, Ckskbb)$

復号された秘密鍵Ksuを用いて放送番組をスクランブルし、放送する。

【0085】利用希望者は自分の秘密鍵Ksuを用いてスクランブルされた放送番組のスクランブルを解除して利用する。このような構成を採ることにより、利用希望者以外の者が番組を利用することは不可能になる。

【0086】このようなシステム構成においてビデオオンデマンド及びペーパービューを実現するシステムとして基本的な構成は図4に示された第4実施例あるいは第5実施例の暗号化システムを利用することができる。放送局31はアナログテレビジョン放送番組の垂直帰線期間の走査線に、あるいは音声帯域の副音声帯域に多重して放送局31の公開鍵Kbbを用いて放送局31の秘密鍵Ksbを暗号化し、

$Ckskbb = E(Kbb, Ksb)$

通信回線37を経由して放送する。

【0087】テレビジョン番組利用希望者38は自分の公開鍵Kbuを通信回線37を経由して放送局31に送信して利用申込を行う。放送局31は放送局の秘密鍵Ksbを用いて放送番組をスクランブルし、通信回線37を経由して放送する。そのとき放送局31の専用鍵Kvbが利用希望者38の公開鍵Kbuで暗号化され

$Ckvbkbu = E(Kbu, Kvb)$

通信回線37を経由して放送される。

【0088】利用希望者38は自分の専用鍵Kvuを用いて放送局31の暗号化専用鍵Ckvbkbuを復号化し、

$Kvb = D(Kvu, Ckvbkbu)$

復号された放送局31の専用鍵Kvbを用いて放送局31の暗号化秘密鍵Ckskbbを復号化し、

$Ksb = D(Kvb, Ckskbb)$

復号された放送局31の秘密鍵Ksbを用いてスクランブルされた放送番組のスクランブルを解除して利用する。

このような構成を採ることにより、利用希望者以外の者

が番組を利用することは不可能になる。

【0089】さらに、この暗号鍵システムは最近盛んに行われているテレビジョン放送と電話とを組み合わせたテレビショッピングにも適用することができる。現在行われているアナログテレビジョン放送を利用したテレビジョンショッキングは、テレビジョン画面に商品紹介と販売方法を表示し、利用者は販売方法に関する情報を手で記録し、記録された情報に基づいて電話を用いて購入申込を行っている。これに対して、本発明の暗号鍵システムにおいてはアナログテレビジョン放送の垂直帰線期間の走査線あるいは音声帯域の副音声帯域に発注書フォーマット、小切手フォーマットのデータを多重して送信することを提案する。一方、パーソナルコンピュータとテレビジョン装置を一体化したパソコンテレビと呼ばれる装置、あるいはＩＣカード、ＰＣカードあるいは挿入ボードとして実現されるビデオキャプチャ装置とパーソナルコンピュータを組み合わせた装置により、テレビジョン画像を取り込むことが行われている。

【0090】これらの発注書フォーマット、小切手フォーマットの多重データとビデオキャプチャ装置を組み合わせることにより電子的にテレビショッキングを行うことができる。このテレビショッキングにおいて、テレビショッキングの商品紹介画面が放送されているときに、垂直帰線期間の走査線あるいは音声帯域の副音声帯域で発注書フォーマット、小切手フォーマットがデータ多重されて放送される。購入を希望する商品の紹介画面が表示されているときに、利用者が操作をすその静止画面とともに発注書フォーマット、小切手フォーマットのデータが取り込まれる。利用者は取り込まれた発注書フォーマット、小切手フォーマットに必要事項を記入し、購入申込を行う。このとき取引の安全性を図るために第１実施例から第５実施例に説明されたシステムにより、公開鍵方式あるいは秘密鍵方式による暗号化及びデジタル署名が行われる。このとき、発注書及び小切手とともに商品紹介の静止画面を添付して購入申込を行うようにすれば、取引内容の確認を行うことができる。

【0091】簡易な方法としては、発注書フォーマット及び小切手フォーマットもテレビジョン画像として送信し、静止画面として取り込まれた発注書フォーマット及び小切手フォーマットに必要事項を記入するようにしてもよい。また、発注書フォーマット及び小切手フォーマットは音声帯域の副音声帯域に多重されるファクシミリ放送で送信することもできる。

【0092】このような方法を採用することにより、テレビショッキングにより、現行のアナログテレビジョン方式によっても電子情報交換（ＥＤＩ）を利用した電子マーケットを実現することができる。

【0093】これらのビデオオンデマンドシステム及び

ペイパービューシステムはアナログテレビジョン放送以外のデジタルテレビジョン放送に対しても適用可能である。通信回線としてＣＡＴＶ回線を使用した場合には放送とデータ通信の双方をこのＣＡＴＶ回線のみによって行うことが可能である。

【0094】また、これらのビデオオンデマンドシステム及びペイパービューシステムは、低速の一般公衆回線あるいは高速のＩＳＤＮ（Integrated Services Digital Network）回線を利用したコンピュータ通信ネットワークシステム、さらには複数のコンピュータ通信ネットワークシステムを接続したインターネットシステムにおいて行われている高品質音声データ及び動画データの送受信に対しても適用可能である。

【0095】使用する装置としてはテレビジョン受信装置に受信装置及び通信装置を組み込むこともできるが、セットトップボックス等を用いて別体に構成することもできる。また、最近徐々に普及しつつあるパーソナルコンピュータとテレビジョン装置を一体化したパソコンテレビと呼ばれる装置、あるいはパーソナルコンピュータにテレビジョン信号を送り込むＩＣカード、ＰＣカードあるいは挿入ボードとして実現されるビデオキャプチャ装置を組み合わせることもできる。

【図面の簡単な説明】

【図１】先願発明の暗号鍵システムの構成図。

【図２】本願発明第１実施例の暗号鍵システムの構成図。

【図３】本願発明第２実施例の暗号鍵システムの構成図。

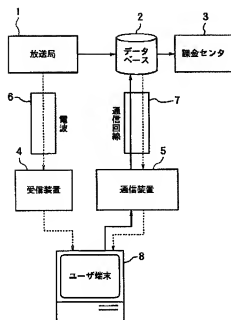
【図４】本願発明第３実施例及び第４実施例の暗号鍵システムの構成図。

【図５】本願発明を応用した第５実施例の構成図。

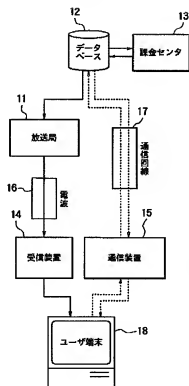
【符号の説明】

- 1, 11 放送局
- 2, 12 データベース
- 3, 13, 23 課金センタ
- 4, 14, 24, 34 受信装置
- 5, 15, 25, 35 データ通信装置
- 6, 16 電波
- 7, 17, 27, 37, 47 通信回線
- 8, 18, 28, 38 ユーザ端末装置
- 21, 31 ＣＡＴＶ局
- 33 管理センタ
- 41 人工衛星
- 42 ユーザ
- 43 小売店
- 44 金融機関
- 45 卸売店

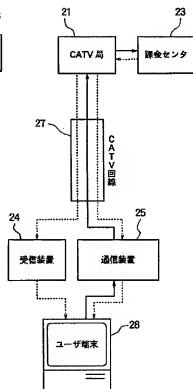
【図1】



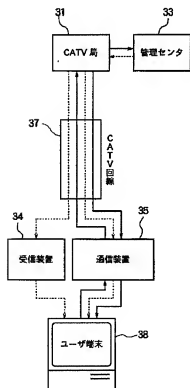
【図2】



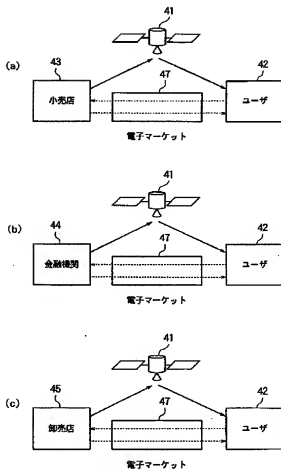
【図3】



【図4】



【図 5】



フロントページの続き

(51) Int. Cl. 6

H 0 4 N 7/167

識別記号

庁内整理番号

8842-5 J

F I

H 0 4 L 9/00

H 0 4 N 7/167

技術表示箇所

6 0 1 F

Z

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-288940

(43)Date of publication of application : 01.11.1996

(51)Int.Cl. H04L 9/08
G06F 15/00
G09C 1/00
H04H 1/00
H04N 7/167

(21)Application number : 07-346095 (71)Applicant : MITSUBISHI CORP

(22)Date of filing : 11.12.1995 (72)Inventor : SAITO MAKOTO
MOMIKI JIYUNICHI

(30)Priority

Priority number : 06309292 Priority date : 13.12.1994 Priority country : JP

(54) CIPHERING KEY SYSTEM

(57)Abstract:

PURPOSE: To prevent illicit use by using a secret key so as to cipher data sending the data to a data communication equipment via a communication channel and decoding the received data through the use of the secret key.

CONSTITUTION: A data communication equipment 15 is used to apply the use of data to a database 12 via a communication channel 17. In this case the user ciphers his own secret key by using an open key of the database 12 and sends the cryptographic key to the database 12. The database 12 decodes the ciphered secret key of the user by using an exclusive key ciphers the data applied for the use by using the secret key of the user to be decoded and sends the ciphered data to the equipment 15 via the channel 17. The user receiving the data ciphered by using his own secret key uses a user terminal equipment 18 to decode the ciphered data ciphered by using his own secret key. Moreover a charge center 13 is provided to the database 12 to be used for account of the charge attending intake/issue of orders.

CLAIMS

[Claim(s)]

[Claim 1] Are an encryption key system which comprises a broadcasting station database, a receiving set, a data communication unit, and installed user terminals, and the aforementioned encryption key system. It is connected between said database and said broadcasting station by off-line means such as online correspondence means such as a dedicated line or a flexible disk, is connected by a communication line between the aforementioned database and said data communication unit, is connected through radio between the aforementioned broadcasting station and said receiving set, and; Are an on-line means directly between said receiving set and said installed user terminals and between said data communication unit and said installed user terminals or it is connected by off-line means such as a flexible disk, and the aforementioned database prepares a public key and a specified key. At said broadcasting station, said public key is supplied and the aforementioned broadcasting station said received public key. When applying for using [which it broadcasts the aforementioned receiving set transmits said received public key to said installed user terminals, the aforementioned installed user terminals save said transmitted public key, and; user wishes] of data, a user's secret key is used and enciphered for said received public key. Said database which transmitted to said database and received a use application of, data decrypts said secret key of said user using said specified key. An encryption key system which data is enciphered using said secret key of said decoded user, it transmits to said data communication unit via said communication line, and the aforementioned user transmits received data to said installed user terminals, and decrypts data using said secret key.

[Claim 2] An encryption key system of the claim 1 by which a digital signature of said database is made by said public key.

[Claim 3] Are an encryption key system which comprises a CATV broadcast office, a charging center, a receiving set, a data communication unit, and installed user terminals, and the aforementioned encryption key system. It is connected by a CATV circuit between said CATV broadcast office and said receiving set, and between said CATV broadcast office and said data communication unit, and directly between the aforementioned receiving set and said installed user terminals and between said data communication unit and said installed user terminals by an on-line means. Or it is connected by off-line means such as a flexible disk, and; user registers a user's public key into a CATV broadcast office beforehand, or show at the time of a use application, and the aforementioned CATV broadcast office enciphers a television program using said secret key of a CATV broadcast office. Encipher a secret key which is a utilization permission key of said CATV broadcast office using a public key of said user who made a use application, broadcast via a CATV circuit, and the aforementioned user receives said television program and said secret key with said receiving set. An encryption key system which decrypts said secret key using a specified key corresponding to said public key, and decrypts a television program with said decoded secret key.

[Claim 4] Are an encryption key system which comprises a CATV broadcast office, a data management center, a receiving set, a data communication unit, and installed

user terminals and the aforementioned encryption key system. By a CATV circuit it is connected between said CATV broadcast office and said data management center by off-line means such as online correspondence means such as a dedicated line or a flexible disk is connected between the; aforementioned CATV broadcast office and said receiving set and between said CATV broadcast office and said data communication unit; it is an on-line means directly between said receiving set and said installed user terminals and between said data communication unit and said installed user terminals — it is — being connected by off-line means such as a flexible disk —; — said data management center a public key and a secret key of each data to supply. Prepare supply said CATV broadcast office and the; aforementioned CATV broadcast office enciphers a secret key of said data management center using a public key of said data management center. While it broadcasts and; user applies for use of data to said data management center via said CATV broadcast office via said CATV circuit using said data communication unit, transmitting said user's public key —; — said data management center each data using said secret key of each data [encipher and] A public key of said data management center is enciphered using said user's public key. Transmit a public key of each enciphered data and said enciphered data management center and a specified key of a data management center to said user and the; aforementioned user decrypts a public key of said data management center using said user's specified key and an encryption key system which decrypts a secret key of each data of said enciphered using a public key of said decrypted data management center and decrypts said data in each using a secret key of each composite-sized data of said.

[Claim 5] An encryption key system of the claim 4 by which a digital signature of said data management center is made by said public key.

[Claim 6] Are an encryption key system which comprises a CATV broadcast office, a data management center, a receiving set, a data communication unit and installed user terminals and the; aforementioned encryption key system. Beforehand register a user's public key into said data management center and the; aforementioned data management center. A public key of said data management center is enciphered using each of said user's public key. A specified key of said data management center. Use and to a public key of said data management center a digital signature. Transmit a public key of said data management center enciphered by carrying out, and a digital signature of said data management center to a CATV broadcast office; the; aforementioned CATV broadcast office broadcasts a public key and a digital signature of said data management center which were enciphered and the; aforementioned user said user's public key. An encryption key system which checks a digital signature using a public key of said decrypted data management center while decrypting an encryption public key of said data management center used and received.

[Claim 7] An encryption key system of the claim 6 which gives a public key of said data management center where user identification information as which each user is not enciphered was enciphered and is broadcast.

[Claim 8] Are an encryption key system which comprises a CATV broadcast office a data management center a receiving set a data communication unit and installed user terminals and the aforementioned encryption key system Said data management center which showed said data management center said user's public key and received a data utilization request from the; aforementioned user whenever a user demanded use of data of said data management center enciphers data by which the utilization request was carried out using said user's public key. An encryption key system by which said user who received said encryption data of which it transmitted to said CATV broadcast office the; aforementioned CATV broadcast office broadcast said received data which was enciphered and; broadcast was done decrypts said encryption data using said user's specified key.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the encryption key system used in the transaction system using television systems database system or electronic intelligence exchange (Electronic Data Interchange: EDI) etc.

[0002]

[Description of the Prior Art] The cable TV broadcast called CATV using the satellite broadcasting coaxial cable or optical cable called a broadcasting satellite (BS) and communications satellite (CS) other than the terrestrial broadcasting usual today called information age is spreading.

[0003] In the satellite broadcasting or CATV broadcast which can distribute several ten channels simultaneously Special channel such as a movie a sport music etc. to which it cannot view and listen depending on a contract comprehensive besides the common channel with which the scramble to which it can view and listen by a comprehensive contract is not applied and by which scramble was carried out are formed. It is necessary to contract but in order [of which scramble is canceled] to view and listen to these channels and to carry out and since this contract term is usually performed in the unit for about one month it cannot view and listen to it by a contract at any time.

[0004] Fee collection is performed while this invention persons obtain a viewing- and-listening permission key from a charging center through a public telephone and telegraph circuit by JP6-46419A and JP6-1410004A The device for it was proposed for the system which cancels the scramble performed with a scramble pattern which is different for every program using a viewing- and-listening permission key and views and listens to a program by JP6-132916A.

[0005] In these systems and devices the program use candidate by whom scramble was done makes a use application to a charging center via a communication line using a communication apparatus and a charging center performs accounting and collects a fee while it transmits a permission key to a communication apparatus to

this use application. The use candidate who received the permission key with the communication apparatus sends a permission key into a receiving set by indirect means such as a direct means or a flexible disk which connects a communication apparatus and a receiving set. The receiving set into which the permission key was sent cancels the scramble of a program with the permission key and a use candidate uses a program.

[0006] To JP6-132916 As an application of these systems and a device, the tape or disk with which two or more data by which scramble was carried out with a respectively different scramble pattern was recorded is sold or lent and the system and device which supply a utilization permission key by an IC card etc. and use specific data are also indicated.

[0007] Each computer until now various kinds of data saved independently today when it is called the information age LAN (Local Area Network) WAN (Wide Area Network) and the Internet system which connected these mutually constitute a computer communication network and the database system used mutually is spreading.

[0008] The television moving image signal which was not able to digitize on the other hand since the amount of information would become huge if it digitizes. By compressing decrease the amount of information and the art which enables practical digitization is developed. Until now, the H.261 standard for a television meeting the JPEG (Joint Photographic image coding Experts Group) standard for still pictures MPEG1 for image storage (Moving Picture) image coding Experts Group 1 standard and the MPEG 2 standard corresponding to the high-definition television broadcast from the present television broadcasting were created.

[0009] The digitization art using such image compression technology is not only used for television broadcasting or video image record but the television video data which was not able to be carried by computer until now can be treated now and the "multi-media system" which deals with simultaneously various kinds of data which a computer treats and the digitized television video data attracts attention as future art. This multi-media system is also included in data communications and is used as one of the data on a database.

[0010] Thus while the use area of a database is expanded by copies or transmission other than how fee collection to the data use on a database is performed and direct use of data etc. How it deals with the problem of the 2nd order copyright generated by the problem of copyright and processing of data to generate poses a big problem. In order to ensure fee collection and processing of copyright it is the best means for it for it to be necessary to carry out as [be / use of data / impossible] if it is not a regular user and to encipher data.

[0011] The information in the various dealings conducted by indicating on paper so far is electronic-data-ized. The electronic market system which performs electronic commerce technology using the electronic intelligence exchange (EDI) mutually transmitted and received using data transmission technology is examined and progressing further and settling an electronic commerce system by electronic banking is also examined. The reliability of a transaction content is required in a

commercial transaction and safety is required in settlement of accounts. Therefore in the electronic commerce system and electronic clearing system with which such reliability and safety are demanded it is necessary to encipher data as an alteration or surreptitious use of data is not performed.

[0012] In these television systems database system or an electronic commerce system in order to encipher data and to decrypt and use the enciphered data an encryption key is required and although an encryption key must be passed to a data user since safety and certainty are required this work is dramatically complicated.

[0013] This invention gives general explanation about data encoding technology first although data encoding technology plays an important role in the composition. It is a case where encipher plaintext data M using the encryption key K and cryptogram data C is obtained in data encoding technology $C=E(KM)$. It is a case where express decrypt cryptogram data C using the encryption key K and plaintext data M is obtained $M=D(KC)$.

It expresses.

[0014] As a typical method used in data encryption there are a private key cryptosystem and a public-key crypto system. A secret key method is a cipher system which uses the same secret key Ks as encryption and decryption.

$$Cmks=E(KsM)$$

$$M=D(KsCmks)$$

[0015] A public key system is an encryption key method with which the key for encryption and the key for decryption are used as an encryption key the key for encryption is exhibited and the key for decryption is not exhibited.

The key for encryption is called the public key Kband the key for decryption is called the specified key Kv.

The side which sends information in order to use this cipher system enciphers plaintext data M using the public key Kb of the side which receives data and is $Cmkb=E(KbM)$.

The side which received data is decrypted using the specified key Kv and obtains plaintext data M.

$$M=D(KvCmkb)$$

The decipherment of a code is dramatically difficult for this public key system.

[0016] As application of data encoding technology in order to secure the reliability of data a digital signature may be performed as an electronic data authentication means. Although there are what uses a secret key and a thing using a public key in a digital signature generally a signature is performed using a public key. By enciphering the document m into which the signer compressed the document M with the hash (Hash) algorithm in the digital signature performed using a public key using a signer's specified key Kva digital signature is obtained and it is $Smkv=E(Kvm)$.

The script M or the compression document m and digital signature Smkv are transmitted to an addressee. An addressee decrypts digital signature Smkv using a signer's public key Kband is $m'=D(KbSmkv)$.

If it is m'=mit will be checked that a signature is right.

[0017] This invention persons proposed the invention entitled an "encryption key system" in prior ***** Japanese Patent Application No. No. 70643 [six to] as a method of passing a user these encryption keys. The encryption key in the encryption key system of this prior invention is passed to an encryption key being passed only to a user in the encryption key system currently generally performed besides a user.

[0018] The composition of the encryption key system proposed by Japanese Patent Application No. No. 70643 [six to] was shown in drawing 1. This system comprises the broadcasting station 1 the database 2 the charging center 3 the receiving set 4 the data communication unit 5 and the installed user terminals 8 which perform multiplexing broadcastssuch as BS-CS and terrestrial televisionor FM or data broadcasting. It is connected by communication linesuch as a dedicated linethe flexible diskor other means between the broadcasting station 1 and the database 2 and between the database 2 and the charging center 3. It is connected by the communication lines 7 such as a public line or a CATV circuitbetween the database 2 and the data communication unit 5. It is connected by the broadcasting electric-wave 6 between the broadcasting station 1 and the receiving set 4. It is connected by direct meanssuch as a connecting cableor indirect meanssuch as a flexible diskbetween the receiving set 4 and the installed user terminals 8 and between the data communication unit 5 and the installed user terminals 8. It is a course of the information which is not enciphered that this figure was shown by the solid lineand the course of the enciphered data was shown by the dashed line.

[0019] In this systemthe database 2 supplies beforehand the utilization permission key Kp (henceforth "a permission key") containing the different encryption key Kd for every data to the broadcasting station 1. In order to make it easy to understandthe permission key Kp is explained as what comprises only the encryption key Kd. It is enciphered using the case where it is supplied without being encipheredand the public encryption key K0and the encryption key Kd is $Ckdk0 = E(K0Kd)$.

It may be supplied as encryption encryption key Ckdk0. When the encryption key Kd is enciphered and suppliedthe public encryption key K0 for decrypting encryption encryption key Ckdk0 is supplied to a user. Supply of this public encryption key K0 may be passed to a user with the encryption data Cmkdwhen the encryption data Cmkd is sentwhen a user registers with a database and it is carried out.

[0020](a) When the encryption key is not enciphered.

In this encryption key systemthe broadcasting station 1 broadcasts the encryption key Kd supplied from the database 2 using the electric wave 6. The receiving set 4 supplies the received encryption key Kd to the installed user terminals 8 and the installed user terminals 8 save the received encryption key Kd at recording mediasuch as semiconductor memorya flexible diskor a hard disk. A data use candidate (user) applies for use of the data M to the database 2 via the

communication line 7 using the data communication unit 5. The database 2 which received the use application of the data M enciphers the data M with use hope using the encryption key Kd which is the permission key Kp and is $Cm_{kd} = E(KdM)$. While transmitting the encryption data Cm_{kd} to a user's data communication unit 5 via the communication line 7 accounting is performed between the charging centers 3. The data communication unit 5 supplies the received encryption data Cm_{kd} to the installed user terminals 8 and the installed user terminals 8 decrypt the encryption data Cm_{kd} using the encryption key Kd saved at the recording medium. $M = D(KdCm_{kd})$

[0021](b) When an encryption key is enciphered and the public encryption key is beforehand distributed to the user.

In this encryption key system when registering that a user uses a database the public encryption key K0 is supplied to a user by recording media such as ROM or a flexible disk and the supplied public encryption key K0 is saved at the installed user terminals 8. The database 2 enciphers the encryption key Kd using the public encryption key K0 and is $Ck_{dk0} = E(K0Kd)$.

Encryption encryption key Ck_{dk0} is supplied to the broadcasting station 1. The broadcasting station 1 broadcasts encryption encryption key Ck_{dk0} supplied from the database 2 using the electric wave 6. The installed user terminals 8 decrypt encryption encryption key Ck_{dk0} using the public encryption key K0 saved beforehand first by supplying encryption encryption key Ck_{dk0} which received to the installed user terminals 8 and the receiving set 4 is $Kd = D(K0Ck_{dk0})$. The decoded encryption key Kd is saved at recording media such as semiconductor memory, a flexible disk or a hard disk.

[0022] A data use candidate applies for use of the data M to the database 2 via the communication line 7 using the data communication unit 5. The database 2 which received the use application of data enciphers the data M with use hope using the encryption key Kd and is $Cm_{kd} = E(KdM)$.

While transmitting to the data communication unit 5 via the communication line 7 accounting is performed between the charging centers 3. The data communication unit 5 supplies the received encryption data Cm_{kd} to the installed user terminals 8 and the installed user terminals 8 decrypt the encryption data Cm_{kd} using the saved encryption key Kd. $M = D(KdCm_{kd})$

[0023](c) When the encryption key is enciphered and a public encryption key is distributed to a user with encryption data.

In this encryption key system the database 2 enciphers the encryption key Kd using the public encryption key K0 and it is $Ck_{dk0} = E(K0Kd)$.

The broadcasting station 1 is supplied. The broadcasting station 1 broadcasts encryption encryption key Ck_{dk0} supplied from the database 2 using the electric wave 6. The receiving set 4 supplies encryption encryption key Ck_{dk0} which received to the installed user terminals 8 and the installed user terminals 8 save encryption encryption key Ck_{dk0} at recording media such as semiconductor memory, a flexible disk or a hard disk.

[0024] A data use candidate applies for use of the data M to the database 2 via the communication line 7 using the data communication unit 5. The database 2 which received the use application of data enciphers the data M with use hope using the encryption key Kd and is $Cm_kd = E(Kd, M)$.

While transmitting to the data communication unit 5 via the communication line 7 together with the public encryption key K0, accounting is performed between the charging centers 3. The installed user terminals 8 decrypt encryption encryption key $Ck_kd, 0$ saved at the recording medium using the public encryption key K0 by supplying the encryption data Cm_kd and the public encryption key K0 which were received to the installed user terminals 8 and the data communication unit 5 is $Kd = D(K0, Ck_kd, 0)$.

The encryption data Cm_kd is decrypted using the decrypted encryption key Kd.
 $M = D(Kd, Cm_kd)$

[0025]

[Summary of the Invention] In this application the concrete composition for applying the invention of the encryption key system indicated to this point ** to television systems, database system or an electronic commerce system is provided. This system comprises a broadcasting station, a database, a receiving set, a data communication unit and installed user terminals. The encryption key which a secret key method and a public key system are adopted as an encryption key method and a digital signature is used further and is used at this time is supplied by broadcast without being enciphered or enciphered. In prevention of the illegal use in database system, a pay-per-view system and a video-on-demand system and management of copyright, this invention is effective and is an effective means in realization of the electronic marketplace which used the electronic intelligence information system further.

[0026]

[Example] Hereafter the example of the invention in this application is described using drawing 2 - drawing 4.

The [1st example] The encryption key system of the 1st example applied to database system was shown the invention in this application in drawing 2 and this system by the multiplexing broadcast or digital broadcasting by BS-CS and terrestrial television or FM broadcasting. Data broadcasting. It comprises the installed user terminals 18 using the receiving set 14 which receives data broadcasting which the broadcasting station 11 to perform the database 12 with which various data containing a video data was stored the charging center 13 and the broadcasting station 11 broadcast the data communication unit 15 which communicates with the database 12 and data.

[0027] It is connected by indirect means such as a direct means or a flexible disk connected by communication lines such as a dedicated line between the database 12 and the broadcasting station 11 and between the database 12 and the charging center 13. It is connected by the communication lines 17 such as a public line or a CATV circuit between the database 12 and the data communication unit 15. It is connected between the broadcasting station 11 and the receiving set 14 by the

electric waves 16 such as terrestrial television broadcasting, satellite TV, JON broadcast, CATV broadcast, FM broadcasting, or satellite data broadcasting. It is connected by direct means such as a connecting cable or indirect means such as a flexible disk between the receiving set 14 and the installed user terminals 18 and between the data communication unit 15 and the installed user terminals 18. It is a course of the data which is not enciphered that this figure was shown by the solid line and the course of the enciphered data was shown by the dashed line. Although delivery of the data between the database 12 and the broadcasting station 11 and between the database 12 and the charging center 13 is performed by a dedicated line or the flexible disk in principle, a public line or a broadcasting satellite, a communications satellite, and terrestrial broadcasting can also perform. In that case, data is enciphered.

[0028] In this system, a secret key method and a public key system are adopted as an encryption key method. The database 12 prepares the public key K_{bd} and the specified key K_{vd} and supplies the public key K_{bd} to the broadcasting station 11. The broadcasting station 11 which received the public key K_{bd} broadcasts the public key K_{bd} by the teletext using the scanning line in the blanking period of an analog television video signal, data broadcasting using the sub voice zone of the analog television audio signal, FM-multiplex-data broadcast, or digital data transmission. The digital signature of the database 11 can be performed to the public key K_{bd} in this case.

[0029] It can also supply for the facilities of the data use to this time without enciphering the table of contents, the contents introduction of data, the commodity catalog, the purchase order, the unindicated check, and copyright information which indicated the title of the data which can be used. The installed user terminals 18 which the receiving set 14 which received the broadcast public key K_{bd} transmitted the public key K_{bd} to the installed user terminals 18 and received the transmitted public key K_{bd} save the public key K_{bd} at recording media such as semiconductor memory, a flexible disk, or a hard disk.

[0030] The user who chose the data which wishes to use applies for use of the data M to the database 12 via the communication line 17 using the data communication unit 15 by table of contents or a contents introduction. At this time, it enciphers using the public key K_{bd} of the database 12 which received its own secret key K_{su} and a user is $Cksuk_{bd} = E(K_{bd}M_{ksu})$.

It transmits to the database 12.

[0031] The database 12 decrypts a user's enciphered secret key $Cksuk_{bd}$ using the specified key K_{vd} and is $K_{su} = D(K_{vd}Cksuk_{bd})$.

It enciphers using the secret key K_{su} of the user who had the data M in which the use application was made, decrypted, and is $Cmksu = E(K_{su}M)$.

It transmits to a user's data communication unit 15 via the communication line 17.

[0032] The user who received the data $Cmksu$ enciphered using its own secret key K_{su} decrypts the encryption data $Cmksu$ which is the installed user terminals 18 and was enciphered using its own secret key K_{su} and is $M = D(K_{su}Cmksu)$.

It uses.

[0033]The charging center 13 interlocked with the database 12 is established in this system. When data is provided for payit is usedbut this charging center 13 is not used when data is data provided for nothing [such as shopping information]. However even if it is data provided for nothing [such as shopping information]it is used when price liquidation accompanying a carrier and order is performed.

[0034]The [2nd example] The encryption key system of the 2nd example that applied the invention in this application to the video-on-demand (Video On Demand:VOD) system which broadcasts a television program according to the hope from a use candidate was shown in drawing 3. This system comprises the CATV broadcast office 21the charging center 23the receiving set 24the data communication unit 25and the installed user terminals 28. When a television program is sponsored for payit is usedbut the charging center 23 is not used when a television program is sponsored for nothing [such as with an advertisement]. In this systemthe television broadcasting program and encryption key which were enciphered are transmitted by CATV circuit 27 which is a single course.

[0035]It is connected between the CATV broadcast office 21 and the charging center 23 by indirect meanssuch as a direct means or a flexible disk electrically connected by communication linessuch as a dedicated line. It is connected by CATV circuit 27 between the CATV broadcast office 21 and the receiving set 24 and between the CATV broadcast office 21 and the data communication unit 25. It is connected by direct meanssuch as a connecting cableor indirect meanssuch as a flexible diskbetween the receiving set 24 and the installed user terminals 28 and between the data communication unit 25 and the installed user terminals 28. It is a course of the data which is not enciphered that this figure was shown by the solid lineand the course of the enciphered data was shown by the dashed line. Although delivery of the data between the CATV broadcast office 21 and the charging center 23 is performed by a dedicated line or the flexible disk in principlea public line or a broadcasting satellite communications satelliteand terrestrial broadcasting can also perform. In that casedata is enciphered.

[0036]In this systema CATV system is also treated as a kind of a database and a secret key method and a public key system are adopted as an encryption key method. The user using this VOD system registers his public key Kbu into the CATV broadcast office 21 beforehandor the communication apparatus 25 is used at the time of a use applicationand he transmits.

[0037]The CATV broadcast office 21 enciphers the secret key Ksb of the CATV broadcast office 21 using the public key Kbu of the transmitted userand is $Cksbkbu=E(KbuKsb)$.

It transmits to the data communication unit 25 via CATV circuit 27. On the other handit is enciphered using the secret key Ksb of the CATV broadcast office 21and the television program M is $Cmksb=E(KsbM)$.

It is broadcast by the receiving set 24 via CATV circuit 27.

[0038]A user decrypts the encryption secret key $Cksbkbu$ of the received CATV broadcast office 21 using a user's specified key Kvuand is $Ksb=D(KvuCksbkbu)$. The encryption television program $Cmksb$ is decrypted using the secret key Ksb of

the decoded CATV broadcast office 21 and it is M=D (KsbCmksb).

It uses.

[0039] This encryption key system is applicable also to television broadcasting audio broadcasts or data broadcasting other than CATV if encryption is possible. The teletext using the scanning line in the blanking period of an analog television video signal data broadcasting using the sub voice zone of the analog television audio signal FM-multiplex-data broadcaster digital data transmission is available as a method of transmitting an encryption key from a broadcasting station.

[0040] Prior ***** Japanese Patent Application No. No. 64889 [six to] as which this invention persons proposed this encryption key system it is available also when distributing an encryption key in the data copyright management system indicated to Japanese Patent Application No. No. 237673 [six to] Japanese Patent Application No. No. 264199 [six to] Japanese Patent Application No. No. 264201 [six to] and Japanese Patent Application No. No. 269959 [six to]. This encryption key system can be applied also when using recording media which this invention persons indicated to JP6-132916A proposed such as CD-ROM on which two or more information is enciphered and recorded by several different patterns. These prior inventions are explained.

[0041] The outline of the data copyright management system indicated to Japanese Patent Application No. No. 64889 [six to] is as follows. In order to manage the copyright in the display (sound-ization is included) of the digital data in database system also including the real time transmission of a digital image preservation a copy processing and transmission Any of the program for managing copyright other than the key which permits use of the data enciphered to the use proposer if needed copyright information or a copyright management message or one or more are transmitted. It manages by supervising so that use which a copyright management message is displayed on a screen when use which applies or is contrary to the contents of permission tends to be performed and performs cautions or warning to a user and applies for a copyright management program is contrary to the contents of permission may not be performed.

[0042] When the whole is respectively supplied with a permission key when the whole is supplied with data a part may be supplied with a permission key and as for a copyright management program copyright information and a copyright management message a part may be supplied with data. For data a permission key a copyright management message copyright information and a copyright management program. When it is in the state which it was transmitted in the state where it was enciphered when a code was solved by utilization time although transmitted in the state where it was enciphered and the code was solved only on the occasion of a display and was enciphered when it was others and not enciphered at all there are three cases of **.

[0043] The outline of the data copyright management system indicated to Japanese Patent Application No. No. 237673 [six to] is as follows. The database with which the data in which this database copyright management system is not

enciphered was storedThe data supplying means which are recording mediasuch as CD-ROM on which the data in which broadcasting stationssuch as Satellite Broadcasters which broadcasts the data enciphered from the databaseor a database was enciphered was recordedIt comprises a communication networka lock management center which manages an encryption keyand a copyright management center which manages the copyright of a databaseThe copyright management program for managing the database use program and copyright for using a databasethe 1st encryption keyand the 2nd encryption key are used. [0044]1 next user registers with a lock management center beforehandin order to use a databaseand the database use program is distributed to him in that case. The program which generates an encryption key peculiar to 1 next user with a predetermined algorithm using the information and information about 1 next user is included in this database use program. When it is it being accumulated in the databasewithout being encipheredbeing broadcastand being recorded on a recording mediumor going via a communication network and is distributedit is enciphered with the 1st encryption keyand let data be encryption data. When distributed via broadcast or a communication networkencryption data The semiconductor memory of 1 next-user terminal unitIt is saved at recording mediasuch as a flexible disk or a hard diskand when it is recorded on a CD-ROM recording medium and distributedit is saved at recording mediasuch as semiconductor memory of a state as it is or 1 next-user terminal unita flexible diskor a hard disk.

[0045]Although a key for 1 next user who uses data directly to decrypt and use encryption data for a lock management center via a communication network from a database is requiredthe information about 1 next user is shown at this time. A lock management center transmits the information about 1 next user to a copyright management centerA copyright management center generates an encryption key peculiar to 1 next user with a predetermined algorithm using the information I about 1 next userenciphers a copyright management programthe 1st encryption keyand the 2nd encryption key using generated 1 next-user encryption keyand transmits them to a lock management center. The copyright management program enciphered using the encryption key generated using the information about this 1 next user is peculiar to 1 next user.

[0046]A copyright management program as which the lock management center which received the enciphered copyright management program was enciphered respectivelyThe 1st encryption key and the 2nd encryption key are transmitted to 1 next-user terminal unit via a communication network to 1 next-user terminal unit1 next user saves the encryption copyright management programthe 1st encryption key of encryptionand the 2nd encryption key of encryption which were received at recording mediasuch as semiconductor memorya flexible diskor a hard disk.

[0047]1 next user generates an encryption key peculiar to 1 next user with a predetermined algorithm using the information about 1 next user using the database use program distributed beforehandAn encryption copyright management

program the 1st encryption key of encryption and the 2nd encryption key of encryption are decrypted using the generated encryption key and encryption data is decrypted using the 1st decoded encryption key.

[0048] Encryption is performed using the 2nd encryption key decoded by the copyright management program decoded when preservation of the data decoded after that copy or transmission was performed. When using the encryption data in which encryption data was saved at recording media such as semiconductor memory in 1 next-user terminal unit, a flexible disk or a hard disk and 1 next user was saved, it decrypts using the 2nd encryption key and this operation is repeated and primary use is performed.

[0049] When it is transmitted to 2 next-user terminal unit via a communication network when encryption data is copied to external storage or the 1st encryption key and the 2nd encryption key are discarded by the copyright management program and it becomes impossible for 1 next user to use encryption data. When encryption data is saved at 1 next-user terminal unit at this time, the information which is not enciphered about 1 next user is added to the encryption data saved.

[0050] When 1 next user uses encryption data again, by having received reissue of the 1st encryption key and the 2nd encryption key from the copyright management center and having performed this reissue, it is checked that 2 next users who received the copy or transmission of encryption data from this 1 next user exist and 2 next users' existence is recorded on a copyright management center.

[0051] 2 next users who received the encryption data copied or transmitted apply for secondary use of encryption data to a copyright management center. Unlike 1 next user, 2 next users do not need to register with a lock management center beforehand and a use application is received by showing a copyright management center the information of 1 next user who received an encryption copy of data or transmission at the time of a use application. Since that user is accepted to be not 2 next users that received an encryption copy of data or transmission from 1 next user but 1 next user when 1 next user information is not shown at this time, that secondary use application is not received. The copyright management center which received the secondary use application transmits the copyright management program which performs re-encryption and the 3rd encryption key for re-decrypting these decryption, re-encryption and re-decryption for the encryption data in which it was decoded for decrypting encryption data, the 2nd encryption key to 2 next users.

[0052] The outline of the copyright management system indicated to Japanese Patent Application No. No. 264199 [six to] is as follows. In this copyright management system, the 2nd specified key corresponding to the 1st specified key corresponding to the 1st public key and the 1st public key which a user prepares, the 2nd public key and the 2nd public key, the 1st secret key that the database side prepares and the 2nd secret key are used.

[0053] In the database side, the data which is not enciphered is enciphered using the 1st secret key. While enciphering the 1st secret key using the 1st public key, the

2nd secret key is enciphered using the 2nd public key and these enciphered data the 1st secret key of encryption and the 2nd secret key of encryption are transmitted to a user.

[0054] While a user decrypts the 1st secret key of encryption using the 1st specified key and decrypts and uses encryption data using the 1st decrypted secret key The 2nd enciphered secret key is decrypted using the 2nd specified key and the 2nd secret key of decryption is used as an encryption key at the time of preservation a copy and transmission of the data after decryption.

[0055] The outline of the data copyright management system indicated to Japanese Patent Application No. No. 264201 [six to] is as follows. When creating new data enciphering and supplying others by processing the enciphered data of the plurality which came to hand from the database the encryption key of two or more data which is raw material and the data which digital-signature-ized the processing program which is a processing process are used as a utilization permission key. If the user who received the data processed and enciphered shows a copyright management center a digital signature and makes a use application Only when a copyright management center checks a processing person based on a digital signature and it is checked that a processing person is a valid user of processing data the encryption key for use is provided to a use proposer.

[0056] The outline of the method indicated to Japanese Patent Application No. No. 269959 [six to] is as follows. Although 1 next user receives decrypts and uses from a database the encryption data as which original data was enciphered with the 1st encryption key After that it is enciphered with the 2nd encryption key generated by the predetermined algorithm combining one or these of the 1st encryption key a primary user datum and the data using frequency and preservation copy and transmission are performed. If 2 next users demand secondary use of data a copyright management center generates the 2nd encryption key with a predetermined algorithm combining one or these of the 1st encryption key of original data a primary user datum and the data using frequency and provides 2 next users with it. 2 next users provided with the 2nd encryption key decrypt and use the original data enciphered using the 2nd encryption key.

[0057] The [3rd example] The encryption key system of the 3rd example that applied the invention in this application to database system or a VOD system was shown in drawing 4. Like [this encryption key system] the encryption key system of the 2nd example shown in drawing 3 of course an encryption key and a television broadcasting program can be passed along a course which is different in these although it passes along the single course which is a CATV circuit. This system comprises the data management centers 33 such as the CATV broadcast office 31 a database or a video system the receiving set 34 the data communication unit 35 and the installed user terminals 38 which perform data broadcasting.

[0058] It is connected between the data management center 33 and the CATV broadcast office 31 by indirect means such as a direct means or a flexible disk connected by communication lines such as a dedicated line. It is connected by

CATV circuit 37 between the CATV broadcast office 31 and the receiving set 34 and between the CATV broadcast office 31 and the data communication unit 35. It is possible to replace with CATV circuit 37 and to use the communication line in which other suitable data broadcasting or data communications are possible. It is connected by direct means such as a connecting cable or indirect means such as a flexible disk between the receiving set 34 and the installed user terminals 38 and between the data communication unit 35 and the installed user terminals 38. It is a course of the data which is not enciphered that this figure was shown by the solid line and the course of the enciphered data was shown by the dashed line. Although delivery of the data between the data management center 33 and the CATV broadcast office 31 is performed by a dedicated line or the flexible disk in principle a public line or a broadcasting satellite communications satellite and terrestrial broadcasting can also perform. In that case data is enciphered.

[0059] The encryption key methods taken in this system are a secret key method and a public key system. The data management center 33 prepares the secret key K_{sdi} which is different by the public key K_{bd} and the specified key K_{vd} common to all the data supplied and the data in each and supplies it to the CATV broadcast office 31. The CATV broadcast office 31 enciphers the received secret key K_{sdi} using the public key K_{bd} of the data management center 33 and is $C_{kdi} = E(K_{bd}, K_{sdi})$.

It broadcasts by the teletext using the scanning line in the blanking period of an analog television video signal, data broadcasting using the sub voice zone of the analog television audio signal, FM-multiplex-data broadcast or digital data transmission. Since use of the table of contents which indicated the title of the data which can be used, data is promoted for the facilities of the data use to this time it can also supply without enciphering the contents introduction explaining the outline of data.

[0060] The user who chose the data which wishes to use applies for use of data to the data management center 33 via the CATV broadcast office 31 via CATV circuit 37 using the data communication unit 35 by the table of contents or a contents introduction. At this time a user transmits his public key K_{bu} to the data management center 33. The data management center 33 which received the use application from a user enciphers the data M using the secret key K_{sdi} and is $C_{mksdi} = E(K_{sdi}, M)$.

It transmits to the installed user terminals 38. The specified key K_{vd} of a data management center is then enciphered using the public key K_{bu} of the user who made a use application and it is $C_{kvdkbu} = E(K_{bu}, K_{vd})$.

It is transmitted to the installed user terminals 38.

[0061] The user who received the encryption specified key C_{kvdkbu} of the data management center decrypts the encryption specified key C_{kvdkbu} of a data management center using a user's specified key K_{vu} and is $K_{vd} = D(K_{vu}, C_{kvdkbu})$. The encryption secret key $C_{ksdikbd}$ is decrypted using the specified key K_{vd} of the decrypted data management center and it is $K_{sdi} = D(K_{vd}, C_{ksdikbd})$.

The encryption data C_{mksdi} is decrypted using the secret key K_{sdi} of the decoded

data management center and it is $M=D$ ($K_{sdi}C_{mksdi}$).

It uses.

[0062]The [4th example] Since the system configuration of the 4th example is the same as the 3rd example shown in drawing 4 explanation is omitted. Although the encryption key methods taken in this system are a secret key method and a public key system like the 3rd example as opposed to the specified key K_{vd} of a data management center being enciphered by the public key K_{bu} of the user who made a use application in the 3rd example and being transmitted to a user as opposed to use of data being distributed to the data M corresponding to an application in the point and the 3rd example which the specified key K_{vd} of a data management center is beforehand distributed using an IC card etc. in the 4th example and are saved in installed user terminals. In the 4th example the data M differs in that it is broadcast by a CATV circuit or satellite broadcasting regardless of use hope.

[0063]When concluding the comprehensive contract that a user uses a data management center and a database the specified key K_{vd} of the data management center common to all the data supplied -- recording media such as an IC card -- or a user is beforehand supplied widely via CATV circuit 37 and it is saved at the semiconductor memory, hard disk drive or flexible disk in the installed user terminals 38. The data management center 33 prepares the secret key K_{sdi} which is different from the public key K_{bd} by the data in each supplied and supplies it to the CATV broadcast office 31. The CATV broadcast office 31 which received the secret key K_{sdi} enciphers the secret key K_{sdi} using the public key K_{bd} and is $C_{ksdi}K_{bd}=E(K_{bd}K_{sdi})$.

It broadcasts by the teletext which used the scanning line in the blanking period of an analog television video signal for the encryption secret key $C_{ksdi}K_{bd}$ data broadcasting using the sub voice zone of the analog television audio signal FM-multiplex-data broadcast or digital data transmission. Since use of the table of contents which indicated the title of the data which can be used or data is promoted for the facilities of the data use to this time it can also supply without enciphering the contents introduction explaining the outline of data.

[0064]The CATV broadcast office 31 enciphers the data M using the secret key K_{sdi} and is $C_{mksdi}=E(K_{sdi}M)$.

On the other hand it broadcasts on a target regardless of use hope by a CATV circuit. A user incorporates into the installed user terminals 38 the data wished to have out of the data currently broadcast by the CATV circuit based on the table of contents or the contents introduction using the receiving set 34.

[0065]A user decrypts the encryption secret key $C_{ksdi}K_{bd}$ using the specified key K_{vd} of the data management center which is distributed beforehand and saved at the semiconductor memory, hard disk drive or flexible disk in the installed user terminals 38 and is $K_{sdi}=D(K_{vd}C_{ksdi}K_{bd})$.

The encryption data C_{mksdi} is decrypted using the decrypted secret key K_{sdi} and it is $M=D(K_{sdi}C_{mksdi})$.

It uses.

[0066]The modification example of others for distributing an encryption key is

described.

The [5th example] In the example described so far the public key Kbd of a data management center is not a communication line course and since it is broadcast from a broadcasting station it cannot be checked whether it is genuine. In such a case the specified key Kvd of a data management center is used for the public key Kbd of a data management center a digital signature is performed and it is $Skbdkvd = E(KvdKbd)$.

Digital signature Skbdkvd is broadcast with the public key Kbd of a data management center. A user checks digital signature Skbdkvd using the received public key Kbd of a data management center and is $Kbd = D(KbdSkbdkvd)$. It will be used if it is genuine.

[0067] The [6th example] When the data management center has adopted the membership system which registers use of a database beforehand in the 5th example the public key Kbu of the user who is the member further is beforehand registered into the data management center. A data management center enciphers the public key Kbd of a data management center using each user's public key Kbu. $Ckdbkbui = E(KbuiKbd)$

The specified key Kvd of a data management center is used for the public key Kbd of a data management center a digital signature is performed and it is $Skbdkvd = E(KvdKbd)$.

Sending the different encryption public key Ckdbkbui for every user and digital signature Skbdkvd to a broadcasting station a broadcasting station broadcasts the received encryption public key Ckdbkbui and digital signature Skbdkvd. At this time if necessary the user identification information as which each user is not enciphered will be given to the encryption public key Ckdbkbui and will be broadcast. The user who received the broadcast encryption public key Ckdbkbui and digital signature Skbdkvd decrypts the encryption public key Ckdbkbui of a data management center using the user's public key Kvui and is $Kbd = D(KvuiCkdbkbui)$.

The public key Kbd of the decrypted data management center is saved in a user's terminal unit. A user checks digital signature Skbdkvd using the received public key Kbd of a data management center and is $Kbd = D(KbdSkbdkvd)$.

The public key Kbd of the data management center saved when it was genuine is used. If it does in this way an encryption key which is different in user each can be distributed.

[0068] The [7th example] Whenever a user accesses a data management center or whenever he requests she shows a data management center his public key Kbu. The data management center which received the request from a user enciphers the demanded data M using a user's public key Kbu and is $Cmkbu = E(KbuM)$.

Sending to a broadcasting station a broadcasting station broadcasts the received encryption data Cmkbu. The user who received the broadcast encryption data Cmkbu decrypts using a user's specified key Kvui and is $M = D(KvuiCmkbu)$. It uses.

[0069] The application which uses the encryption key system of the invention in

this application is shown using drawing 5. To the electronic marketplace dealings using an electronic information exchange system each application shown in this figure. It is the composition at the time of applying these encryption key systems to the wholesale distribution which a maker etc. perform respectively that it was shown in the settlement of accounts by an electronic check at (c) that what was shown in (a) was shown in the credit settlement which a retail store performs at (b). In addition to a secret key method a digital signature is used and these systems comprise the wholesale shop 45 which is the retail store 43 the financial institution 44 or a maker etc. which is a WWW (World Wide Web) server on the user 42 and the Internet.

[0070] The [8th example] In the credit settlement in the retail store shown in (a) The retail store 43 broadcasts the data Ms of the format of a purchase order a credit card format an advertisement a catalog a preview a product description the contents introduction of a database a table of contents / price list / price list etc. via the satellite 41 or a CATV circuit. The user 42 who received the public key Kbs of the data Ms of a purchase-order format etc. and the retail store 43 enciphers a user's secret key Ksu using the public key Kbs of the retail store 43 and is $Cksukbs = E(KbsKsu)$.

Based on information including an advertisement a catalog a product description a fee price list etc. the user's 42 secret key Ksu is used for a purchase order it enciphers to it the matters Musuch as an order content an amount paid and a credit card number are written down in it and it is $Cmuksu = E(KsuMu)$.

The matter Mu is set to compression document mu if needed a digital signature is performed using the user's 42 specified key Kvu and it is $Smukvu = E(KvuMu)$.

The user's 42 public key Kbu is attached and it transmits to the retail store 43 via the network 47.

[0071] The retail store 43 which received the purchase order etc. decrypts the user's 42 encryption secret key Cksukbs using the specified key Kvs of the retail store 43 and is $Ksu = D(KvsCksukbs)$.

The encryption purchase order Cmuksu is decrypted using the user's 42 decrypted secret key Ksu and it is $Mu = D(KsuCmuksu)$.

A processing order is performed. The user's 42 digital signature Smukvu is checked using the public key Kbu which the user 42 furthermore attached and it is $mu = D(KbuSmukvu)$.

A receipt is replied to the user 42 via the network 47. In this system since the credit card number as which a purchase order is filled in is enciphered and sent surreptitious use of a credit number can be prevented.

[0072] The retail store 43 A purchase-order format a credit card format Digital data Ms1 such as an advertisement a catalog a preview a product description a contents introduction of a database a table of contents / price list / price list is set to compression document ms1 the specified key Kvs of the retail store 43 is used for this a digital signature is performed and it is $Sms1kvs = E(Kvmsms1)$.

attach and broadcast the public key Kbs of the retail store 43 and a user uses the public key Kbs of the retail store 43 — digital signature $Sms1kvs$ — check $ms' = D$

(KbsSmskvs)

By being made to carry outdealings will become more positive.

[0073]The [9th example] In the settlement of accounts by the electronic check shown in (b)the financial institution 44 attaches the public key Kbf of the financial institution 44 to the unindicated check format Mf which is digital dataand broadcasts via the satellite 41 or a CATV circuit. The user 42 who received the unindicated check format Mf enciphers the user's 42 secret key Ksu using the public key Kbf of a financial institutionand is Cksukbf=E (KbfKsu).

The matter Mu about a payee and an amount paid is enciphered and filled in using the user's 42 secret key Ksuand it is Cmuksu=E (KsuMu).

The matter Mu is set to compression document mu if neededthe user's 42 specified key Kvu is used for thisa digital signature is performedand it is Smukvu=E (Kvumu).

The user's 42 encryption secret key Cksukbf enciphered by the user's 42 public key Kbu and the public key Kbf of the financial institution 44 is attachedand it transmits to the financial institution 44 via the network 47.

[0074]The financial institution 44 which received the indicated check decrypts the user's 42 encryption secret key Cksukbf using the specified key Kvf of a financial institutionand is Ksu=D (KvfCksukbf).

The encryption data Cmuksu of a payee and an amount paid is decrypted using a user's decrypted secret key Ksuand it is Mu=D (KsuCmuksu).

The indicated contents are checked and currency conversion processing is performed. What furthermore has digital signature Smukvu checks the user 42 using the public key Kbu which the user 42 attachedand is mu'=D (KbuSmukvu). It enciphers using the public key Kbu to which the user 42 attached written confirmation Ms2and is Cms2 kbu=E (KbuMs2).

It replies to the user 42 via the network 47.

[0075]The user who received encryption written confirmation Cms2kbu from the financial institution 44 decrypts encryption written confirmation Cms2kbu using the user's 42 specified key Kvuand is Ms2=D (KvuCms2kbu).

The contents are checked. According to this systemsince the payee and the amount paid were enciphered and the check is filled ininsurreptitious use of the contents indicated to the check can be prevented.

[0076]The unindicated check format Mf which is digital data is used as the compression document mfthe specified key Kvf of the financial institution 44 is used for thisa digital signature is performedand it is Smfkvf=E (Kvfmf).

The public key Kbf of the financial institution 44 is attached and broadcasta user uses the public key Kbf of the financial institution 44and it is check mf=D (KbfSmfkvf) about digital signature Smskfvf.

Smskbu=E which performs a digital signature using the public key Kbu which was made to carry outand used the written confirmation Ms as the compression document ms furtherand the user attached to this (Kbums)

By making it likea financial institution can check an entry person.

[0077]The [10th example] In the wholesale shops 45such as a maker by which it

was shown to (c) the wholesale shop 45 sets request-for-quotation format Mw1 to compressed data mw1 the specified key Kvw of the wholesale shop 45 is used for this a digital signature is performed and it is $Smw1\ kvw=E(Kvw mw1)$.

The public key Kbw of the wholesale shop 45 is attached and it broadcasts via the satellite 41 or a CATV circuit. The user 42 who is the retail store which received the public key Kbw of request-for-quotation format Mw1 broadcast and the wholesale shop 45 enciphers the request for quotation Mu using the public key Kbw of the wholesale shop 45 and is $Cmukbw=E(Kbw Mu)$.

It transmits to the wholesale shop 45 via the network 47. At this time the request for quotation Mu is set to compressed data mu if needed the user's 42 specified key Kvu is used for this a digital signature is performed and it is $Smkvu=E(Kvumu)$. It transmits to the wholesale shop 45 with the user's 42 public key Kbu.

[0078] The wholesale shop 45 which received the encryption request for quotation $Cmukbw$ decrypts the encryption request for quotation $Cmukbw$ using the specified key Kvw of the wholesale shop 45 and is $Mu=D(Kvu Cmukbw)$.

The indicated contents Mu of a request for quotation are checked and an estimate is performed. When digital signature $Smkvu$ is furthermore carried out a digital signature is checked using the public key Kbu of the transmitted user 42 and it is $mu=D(Kbu Smkvu)$.

A request for quotation is checked. The wholesale shop 45 which performed the estimate enciphers estimate Mw2 using the user's 42 public key Kbu and is $Cmw2\ kbu=D(Kbu Mw2)$.

It transmits to the user 42 via the network 47.

[0079] The user 42 who received encryption estimate $Cmw2\ kbu$ of the wholesale shop 45 decrypts using the user's 42 specified key Kvu.
 $Mw2=D(Kvu Cm2\ kbu)$

According to this system since the public key and the specified key are used there is no possibility that the contents of the estimate may be plagiarized and a different estimate for every user can be performed.

[0080] These (a) In the system shown in - (c) since the various formats and advertisement which do not require confidentiality are broadcast by satellite broadcasting or CATV broadcast data can be transmitted effectively.

[0081] As explained above The multimedia system which united general information media such as television broadcasting or audio broadcast which has so far existed as a system independently and the data-communications media using a computer is realizable by using the encryption key system of this invention. Hereafter the concrete composition which realized the multimedia system is explained.

[0082] The present television broadcasting is performed by terrestrial broadcastingsatellite broadcasting or CATV broadcast by an analog form and the other hand most general data telecommunication line is a public line using an electric wire. The composition fundamental as a system which realizes a video on demand in such a system configuration can use the encryption key system of the 1st example shown in drawing 2, a broadcasting station -- the scanning line of the vertical-retrace-line period of an analog television broadcasting program -- or

multiplex is carried out to the sub voice zone of a voice band and the public key K_{bb} of a broadcasting station is broadcast.

[0083] It enciphers using the public key K_{bb} of the broadcasting station which has its own secret key K_{su} broadcast and a television program use candidate is $Cksk_{bb}=E(K_{bb}K_{su})$.

The encryption secret key $Cksk_{bb}$ is transmitted to a broadcasting station via a communication line and a use application is made.

[0084] A broadcasting station decrypts a use candidate's encryption secret key $Cksk_{bb}$ using the specified key K_{vb} of a broadcasting station and is $K_{su}=D(K_{vb}Cksk_{bb})$.

Using the decoded secret key K_{su} the scramble of the program is carried out and it is broadcast.

[0085] A use candidate cancels and uses the scramble of the program by which scramble was carried out using its own secret key K_{su} . By taking such composition it becomes impossible for persons other than a use candidate to use a program.

[0086] The composition fundamental as a system which realizes a video on demand and pay-per-view in such a system configuration can use the encryption key system of the 4th example or the 5th example shown in drawing 4. Multiplex is carried out to the scanning line of the vertical-retrace-line period of an analog television broadcasting program or the sub voice zone of a voice band the secret key K_{sb} of the broadcasting station 31 is enciphered using the public key K_{bb} of the broadcasting station 31 and the broadcasting station 31 is $Cksk_{bb}=E(K_{bb}K_{sb})$. It broadcasts via the communication line 37.

[0087] The television program use candidate 38 transmits his public key K_{bu} to the broadcasting station 31 via the communication line 37 and makes a use application. The broadcasting station 31 carries out the scramble of the program using the secret key K_{sb} of a broadcasting station and broadcasts it via the communication line 37. The specified key K_{vb} of the broadcasting station 31 is then enciphered by the use candidate's 38 public key K_{bu} and it is $Ckvbk_{bu}=E(K_{bu}K_{vb})$. It is broadcast via the communication line 37.

[0088] The use candidate 38 decrypts the encryption specified key $Ckvbk_{bu}$ of the broadcasting station 31 using his own specified key K_{vu} and is $K_{vb}=D(K_{vu}Ckvbk_{bu})$.

The encryption secret key $Cksk_{bb}$ of the broadcasting station 31 is decrypted using the specified key K_{vb} of the decoded broadcasting station 31 and it is $K_{sb}=D(K_{vb}Cksk_{bb})$.

The scramble of the program by which scramble was carried out using the secret key K_{sb} of the decoded broadcasting station 31 is canceled and used. By taking such composition it becomes impossible for persons other than a use candidate to use a program.

[0089] This encryption key system is applicable also to the TV shopping which combined the television broadcasting performed briskly these days and a telephone. Television shopping using the analog television broadcasting performed

now displays an article introduction and a sales method on a television screen and a user records the information about a sales method by hand and is performing purchase applying using the telephone based on the recorded information. On the other hand it proposes carrying out multiplex [of the data of a purchase-order format and a check format] to the scanning line of the vertical-retrace-line period of analog television broadcasting the sub voice zone of a voice band and transmitting to it in the encryption key system of this invention. A device called the personal computer television which unified the personal computer and the TV apparatus on the other hand or incorporating a television picture is performed by the video capture device realized as an IC card or a PC card or an insertion board and the device which combined the personal computer.

[0090] TV shopping can be electronically performed by combining the data multiplex and video capture device of these purchase-order formats and a check format. In this TV shopping when the article introduction picture of TV shopping is broadcast by the scanning line of a vertical-retrace-line period or the sub voice zone of a voice band data multiplex [of a purchase-order format and the check format] is carried out and they are broadcast. When the introduction screen of the goods which wish to purchase is displayed if a user operates it the data of a purchase-order format and a check format will be incorporated with the still picture side. A user writes down necessary information in the purchase-order format and check format which were incorporated and performs purchase applying. The encryption and the digital signature by the public key system or a secret key method are performed by the system explained to the 5th example from the 1st example in order to plan the safety of dealings at this time. A transaction content can be checked if the still picture side of an article introduction is attached and it is made to perform purchase applying with a purchase order and a check at this time.

[0091] A purchase-order format and a check format also transmit as a television picture and it may be made to write down necessary information in the purchase-order format and check format which were incorporated as a still picture side as a simple method. A purchase-order format and a check format can also be transmitted by the TV broadcast through facsimile by which multiplex is carried out to the sub voice zone of a voice band.

[0092] By adopting such a method the electronic marketplace which used electronic intelligence exchange (EDI) also with the present analog television system is realizable by TV shopping.

[0093] These video-on-demand systems and a pay-per-view system are applicable also to digital television broadcasting other than analog television broadcasting. When a CATV circuit is used as a communication line it is possible to perform the both sides of broadcast and data communications only by this CATV circuit.

[0094] These video-on-demand systems and a pay-per-view system The online-communications network system using a low-speed ordinary public circuit or high-speed ISDN (Integrated Services Digital Network) circuit it is applicable also to the transmission and reception of quality voice data and a video data currently

performed in the Internet system which connected further two or more online-communications network systems.

[0095] Although a receiving set and a communication apparatus are also incorporable into a television system as a device to be used it can also constitute in a different body using a set top box etc. A device called the personal computer television which unified the personal computer which has been spreading gradually recently and the TV apparatus Or it can also constitute combining the video capture device realized as the IC card which sends a television signal into a personal computer a PC card or an insertion board.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The lineblock diagram of the encryption key system of a prior invention.

[Drawing 2] The lineblock diagram of the encryption key system of the 1st example of the invention in this application.

[Drawing 3] The lineblock diagram of the encryption key system of the 2nd example of the invention in this application.

[Drawing 4] The lineblock diagram of the encryption key system of the 3rd example of the invention in this application and the 4th example.

[Drawing 5] The lineblock diagram of the 5th example adapting the invention in this application.

[Description of Notations]

1 and 11 Broadcasting station

2 and 12 Database

31323 charging centers

41424 and 34 Receiving set

5152535 data communication units

6 and 16 Electric wave

7172737 and 47 Communication line

8182838 installed user terminals

2131 CATV stations

33 Control center

41 Artificial satellite

42 User

43 Retail store

44 Financial institution

45 Wholesale shop
